



---

Junos<sup>®</sup> OS

# Services Interfaces Configuration Guide

Release

14.1



---

Published: 2014-05-28

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Junos<sup>®</sup> OS Services Interfaces Configuration Guide*  
Release 14.1  
Copyright © 2014, Juniper Networks, Inc.  
All rights reserved.

Revision History  
April, 2014—Junos OS 14.1

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Abbreviated Table of Contents

	About This Guide .....	xlix
Part 1	Overview	
Chapter 1	Services Interfaces Overview .....	3
Chapter 2	Services Interfaces Configuration Statements .....	7
Part 2	Adaptive Services	
Chapter 3	Adaptive Services Overview .....	39
Chapter 4	Applications Configuration Guidelines .....	125
Chapter 5	Summary of Applications Configuration Statements .....	179
Chapter 6	Network Address Translation Configuration Guidelines .....	191
Chapter 7	Summary of Network Address Translation Configuration Statements ..	305
Chapter 8	Softwire Configuration Guidelines .....	343
Chapter 9	Summary of Softwire Services Configuration Statements .....	367
Chapter 10	Network Address Translation and Softwire Administration .....	373
Chapter 11	Stateful Firewall Services Configuration Guidelines .....	387
Chapter 12	Summary of Stateful Firewall Configuration Statements .....	397
Chapter 13	Stateful Firewall on the Embedded Junos OS Platform Configuration Guidelines .....	409
Chapter 14	Summary of Stateful Firewall on the Embedded Junos OS Platform Configuration Statements .....	413
Chapter 15	Load Balancing Configuration Guidelines .....	425
Chapter 16	Summary of Load Balancing Configuration Statements .....	431
Chapter 17	Intrusion Detection Service Configuration Guidelines .....	445
Chapter 18	Summary of Intrusion Detection Service Configuration Statements ....	457
Chapter 19	IPsec Services Configuration Guidelines .....	479
Chapter 20	Summary of IPsec Services Configuration Statements .....	535
Chapter 21	Layer 2 Tunneling Protocol Services Configuration Guidelines .....	577
Chapter 22	Summary of Layer 2 Tunneling Protocol Configuration Statements ....	597
Chapter 23	Link Services IQ Interfaces Configuration Guidelines .....	615
Chapter 24	Summary of Link Services IQ Configuration Statements .....	681
Chapter 25	Voice Services Configuration Guidelines .....	695
Chapter 26	Summary of Voice Services Configuration Statements .....	705

Chapter 27	Class-of-Service Configuration Guidelines . . . . .	715
Chapter 28	Summary of Class-of-Service Configuration Statements . . . . .	725
Chapter 29	Service Set Configuration Guidelines . . . . .	741
Chapter 30	Summary of Service Set Configuration Statements . . . . .	761
Chapter 31	Service Interface Configuration Guidelines . . . . .	795
Chapter 32	Summary of Service Interface Configuration Statements . . . . .	813
Chapter 33	PGCP Configuration Guidelines for the BGF Feature . . . . .	837
Chapter 34	Summary of PGCP Configuration Statements . . . . .	843
Chapter 35	Service Interface Pools Configuration Guidelines . . . . .	949
Chapter 36	Summary of Service Interface Pools Statements . . . . .	951
Chapter 37	PTSP Configuration Guidelines . . . . .	953
Chapter 38	Summary of PTSP Configuration Statements . . . . .	955
Part 3	Junos Application Aware	
Chapter 39	Junos Application Aware Overview . . . . .	979
Chapter 40	Application Identification Configuration Guidelines . . . . .	993
Chapter 41	Summary of Application Identification Configuration Statements . . . . .	1013
Chapter 42	Application-Aware Access List Configuration Guidelines . . . . .	1057
Chapter 43	Summary of AACL Configuration Statements . . . . .	1067
Chapter 44	Local Policy Decision Function Configuration Guidelines . . . . .	1079
Chapter 45	Summary of L-PDF Configuration Statements . . . . .	1087
Part 4	Encryption Services	
Chapter 46	Encryption Overview . . . . .	1099
Chapter 47	Encryption Interfaces Configuration Guidelines . . . . .	1101
Chapter 48	Summary of Encryption Configuration Statements . . . . .	1111
Part 5	Flow Monitoring and Discard Accounting Services	
Chapter 49	Flow Monitoring and Discard Accounting Overview . . . . .	1123
Chapter 50	Flow Monitoring and Discard Accounting Configuration Guidelines . . . . .	1129
Chapter 51	Summary of Flow-Monitoring Configuration Statements . . . . .	1213
Chapter 52	Flow Collection Configuration Guidelines . . . . .	1295
Chapter 53	Summary of Flow Collection Configuration Statements . . . . .	1309
Chapter 54	Dynamic Flow Capture Configuration Guidelines . . . . .	1327
Chapter 55	Flow-Tap Configuration Guidelines . . . . .	1339
Chapter 56	Summary of Dynamic Flow Capture and Flow-Tap Configuration Statements . . . . .	1349
Part 6	Link and Multilink Services	
Chapter 57	Link and Multilink Services Overview . . . . .	1371

Chapter 58	Link and Multilink Services Configuration Guidelines . . . . .	1375
Chapter 59	Summary of Multilink and Link Services Configuration Statements . . . .	1441
Part 7	Real-Time Performance Monitoring Services	
Chapter 60	Real-Time Performance Monitoring Services Overview . . . . .	1467
Chapter 61	Real-Time Performance Monitoring Configuration Guidelines . . . . .	1471
Chapter 62	Summary of Real-Time Performance Monitoring Configuration Statements . . . . .	1521
Part 8	Tunnel Services	
Chapter 63	Tunnel Services Overview . . . . .	1563
Chapter 64	Tunnel Interfaces Configuration Guidelines . . . . .	1567
Chapter 65	Summary of Tunnel Services Configuration Statements . . . . .	1591
Part 9	Index	
	Index . . . . .	1609
	Index of Statements and Commands . . . . .	1635



# Table of Contents

	<b>About This Guide</b> .....	<b>xlix</b>
	Junos Documentation and Release Notes .....	xlix
	Objectives .....	l
	Audience .....	l
	Supported Platforms .....	l
	Using the Indexes .....	li
	Using the Examples in This Manual .....	li
	Merging a Full Example .....	li
	Merging a Snippet .....	lii
	Documentation Conventions .....	lii
	Documentation Feedback .....	liv
	Requesting Technical Support .....	lv
	Self-Help Online Tools and Resources .....	lv
	Opening a Case with JTAC .....	lv
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Services Interfaces Overview</b> .....	<b>3</b>
	Understanding Services PICs .....	3
	Adaptive services and Multiservices PICs .....	3
	Encryption Services (ES) PIC .....	4
	Multilink Services and Link Services PICs .....	4
	Monitoring Services PICs .....	4
	Tunnel Services PIC .....	5
	Multiservices MIC and Multiservices MPC .....	5
	Supported Platforms .....	5
<b>Chapter 2</b>	<b>Services Interfaces Configuration Statements</b> .....	<b>7</b>
	[edit applications] Hierarchy Level .....	7
	[edit forwarding-options] Hierarchy Level .....	8
	[edit interfaces] Hierarchy Level .....	10
	[edit logical-systems] Hierarchy Level .....	14
	[edit services] Hierarchy Level .....	14

## Part 2

## Chapter 3

## Adaptive Services

<b>Adaptive Services Overview</b>	<b>39</b>
Adaptive Services Overview	39
Enabling Service Packages	41
Layer 2 Service Package Capabilities and Interfaces	45
Services Configuration Procedure	46
Packet Flow Through the Adaptive Services or Multiservices PIC	47
Junos Network Secure Overview	48
Stateful Firewall Support for Application Protocols	49
Stateful Firewall Anomaly Checking	50
Junos Address Aware Network Addressing Overview	51
Sample IPv6 Transition Scenarios	52
Example 1: IPv4 Depletion with a Non-IPv6 Access Network	52
Example 2: IPv4 Depletion with an IPv6 Access Network	52
Example 3: IPv4 Depletion for Mobile Networks	53
Junos OS CGNAT Implementation Overview	53
Network Address Translation Overview for MS-DPC, MS-MPC, and MS-MIC	
Line Cards	54
Types of NAT	54
Inline Network Address Translation Overview for MPC Types 1, 2, and 3	59
Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card	60
ALGs Available by Default for Junos OS Address Aware NAT	62
Port Control Protocol Overview	64
Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card	66
ALGs Available by Default for Junos OS Address Aware NAT	69
Tunneling Services for IPv4-to-IPv6 Transition Overview	71
6to4 Overview	72
Basic 6to4	72
6to4 Anycast	73
6to4 Provider-Managed Tunnels	73
DS-Lite Softwires—IPv4 over IPv6	74
6rd Softwires—IPv6 over IPv4	74
Understanding Junos VPN Site Secure	75
IPsec	76
Security Associations	76
IKE	77
Comparison of IPsec on ES PICs and Junos VPN Site Secure on Multiservices Line Cards	77
Layer 2 Tunneling Protocol Overview	78
Voice Services Overview	79
HTTP URL Tracking and Policy Control for Client Requests	79
Guidelines for Configuring HTTP URL Monitoring for Client Requests	80
Configuring HTTP URL Tracking and Policy Control	81

	Class of Service Overview .....	82
	Configuring Routing Services on Multiservices MIC and MPC (MS-MIC and MS-MPC) .....	82
	Key Features Supported on Multiservices MIC and MPC (MS-MIC and MS-MPC) .....	83
	Junos Address Aware on MS-MIC and MS-MPC .....	84
	Junos VPN Site Secure Support on the MS-MIC and MS-MPC .....	84
	Junos Traffic Vision Support on MS-MIC and MS-MPC .....	85
	Aggregated Multiservices (AMS) Interface Support on MS-MIC .....	85
	Example: Configuring Flow Monitoring on MS-MIC and MS-MPC .....	86
	Understanding Aggregated Multiservices Interfaces .....	93
	Aggregated Multiservices Interface .....	93
	Member Failure Options and High Availability Settings .....	93
	Example: Configuring an Aggregated Multiservices Interface (AMS) .....	94
	Example: Configuring Next-Hop Style Services on an Aggregated Multiservices Interface .....	99
	Example: Configuring Junos VPN Site Secure on MS MIC and MS-MPC ....	102
	Example: NAPT Configuration for the MS-MPC .....	113
	Examples: Services Interfaces Configuration .....	117
	Example: Service Interfaces Configuration .....	118
	Example: Virtual Routing and Forwarding (VRF) and Service Configuration .....	121
	Example: Dynamic Source NAT as a Next-Hop Service .....	122
	Example: BOOTP and Broadcast Addresses .....	123
<b>Chapter 4</b>	<b>Applications Configuration Guidelines .....</b>	<b>125</b>
	ALG Descriptions .....	126
	Supported ALGs .....	126
	ALG Support Details .....	127
	Basic TCP ALG .....	128
	Basic UDP ALG .....	128
	BOOTP .....	129
	DCE RPC Services .....	129
	DNS .....	129
	FTP .....	129
	H323 .....	130
	ICMP .....	130
	IIOIP .....	130
	IP .....	131
	NetBIOS .....	131
	NetShow .....	131
	ONC RPC Services .....	131
	PPTP .....	131
	RealAudio .....	132
	Sun RPC and RPC Portmap Services .....	132
	RTSP .....	134
	SIP .....	134
	SNMP .....	135
	SQLNet .....	135

TFTP	135
Traceroute	135
UNIX Remote-Shell Services	136
Winframe	136
Juniper Networks Defaults	136
Configuring Application Protocol Properties	146
Configuring an Application Protocol	147
Configuring the Network Protocol	149
Configuring the ICMP Code and Type	150
Configuring Source and Destination Ports	152
Configuring the Inactivity Timeout Period	155
Configuring SIP	155
SIP ALG Interaction with Network Address Translation	156
Junos OS SIP ALG Limitations	162
Configuring an SNMP Command for Packet Matching	162
Configuring an RPC Program Number	163
Configuring the TTL Threshold	163
Configuring a Universal Unique Identifier	163
Configuring Application Sets	163
Verifying the Output of ALG Sessions	164
FTP Example	164
Sample Output	164
FTP System Log Messages	165
Analysis	166
Troubleshooting Questions	166
RTSP ALG Example	167
Sample Output	167
Analysis	167
Troubleshooting Questions	167
System Log Messages	169
System Log Configuration	169
System Log Output	170
Junos Default Groups	170
Examples: Referencing the Preset Statement from the Junos Default Group	175
Examples: Configuring Application Protocols	177
<b>Chapter 5</b>	
<b>Summary of Applications Configuration Statements</b>	<b>179</b>
application	180
application-protocol	181
application-set	182
applications	183
destination-port	184
icmp-code	185
icmp-type	185
inactivity-timeout	186
learn-sip-register	186
protocol	187
rpc-program-number	188

---

Copyright © 2014, Juniper Networks, Inc. xi

Configuring Dynamic Source Address and Port Translation for IPv6 Networks	233
Configuring Secured Port Block Allocation	235
Configuring Deterministic Port Block Allocation	237
Configuring Stateful NAT64	238
Configuring Protocol Translation Between IPv6 and IPv4 Networks - NAT-PT	240
Configuring the DNS ALG Application	240
Configuring the NAT Pool and NAT Rule	241
Configuring the Service Set for NAT	244
Configuring Trace Options	245
Example: Assigning Addresses from a Dynamic Pool for Static Use	246
Example: Configuring NAT for Multicast Traffic	247
Rendezvous Point Configuration	247
Router 1 Configuration	250
Configuring Port Forwarding for Static Destination Address Translation	251
Configuring Port Forwarding Without Destination Address Translation	254
Example: Configuring Port Forwarding with Twice NAT	255
Configuring Port Control Protocol	257
Configuring PCP Server Options	257
Configuring a PCP Rule	258
Configuring a Service Set to Apply PCP	259
SYSLOG Message Configuration	259
Example: NAT 44 CGN Configurations	259
Example: NAPT Configuration for the MS-MPC	263
Example: Configuring NAT-PT	267
Example: Configuring Inline Network Address Translation - Interface-Service	282
Service Set	282
Port Control Protocol Configuration Examples	290
Example: Configuring Port Control Protocol with NAPT44	290
Carrier-Grade NAT Implementation: Best Practices	296
Use APP and Round-Robin Address-Allocation	296
Do Not Use EIM with SIP	297
Do Not Use EIM with HTTP, DNS, or When Not Needed	297
Define PBA Blocks Based on User Profiles	298
Do Not Change the PBA Configuration on Running Systems	299
Do Not Allocate Excessively Large NAT Pools	300
Configure the System Log for PBA Only When Needed	300
Use Redundant Service PIC (RSP) Interfaces for Failover	302
Contain the Effects of Missing IP Fragments	303
Do Not Use Configurations Prone to Routing Loops	303
<b>Chapter 7 Summary of Network Address Translation Configuration Statements</b>	<b>305</b>
address (Services NAT Pool)	307
address-allocation	307
address-range	308
allow-overlapping-nat-pools	308
app-mapping-timeout	309
application-sets (Services NAT)	309

applications (Services NAT) .....	310
cgn-pic .....	310
destination-address .....	311
destination-address-range .....	312
destination-pool .....	312
destination-port range .....	313
destination-prefix .....	313
destination-prefix-list .....	314
destined-port .....	314
deterministic-port-block-allocation .....	315
dns-alg-pool .....	316
dns-alg-prefix .....	316
ei-mapping-timeout .....	317
eif-flow-limit .....	317
from (Services NAT) .....	318
ipv6-multicast-interfaces .....	319
mapping-refresh .....	319
mapping-timeout .....	320
match-direction .....	320
no-translation .....	321
overload-pool .....	321
overload-prefix .....	322
pool .....	323
port .....	324
port-forwarding .....	325
port-forwarding-mappings .....	325
ports-per-session .....	326
rule .....	327
rule-set .....	328
secure-nat-mapping .....	328
secured-port-block-allocation .....	329
server (pcp) .....	330
services (NAT) .....	331
service-set (Services) .....	332
source-address (NAT) .....	334
source-address-range .....	334
source-pool .....	335
source-prefix .....	335
source-prefix-list .....	336
syslog .....	336
translated-port .....	337
term .....	338
then .....	339
translated .....	340
translation-type .....	341
<b>Chapter 8</b>	
<b>Software Configuration Guidelines .....</b>	<b>343</b>
Configuring a DS-Lite Software Concentrator .....	343
Configuring a 6rd Software Concentrator .....	344

	Configuring Stateful Firewall Rules for 6rd Software . . . . .	345
	Configuring Software Rules . . . . .	345
	Configuring Service Sets for Software . . . . .	346
	Example: Basic DS-Lite Configuration . . . . .	347
	Example: Basic 6rd Configuration . . . . .	353
	Example: Configuring DS-Lite and 6rd in the Same Service Set . . . . .	358
	Configuring a 6to4 Provider-Managed Tunnel . . . . .	364
<b>Chapter 9</b>	<b>Summary of Software Services Configuration Statements . . . . .</b>	<b>367</b>
	ds-lite . . . . .	368
	rule (Software) . . . . .	369
	rule-set (Software) . . . . .	369
	software-concentrator . . . . .	370
	software-rules . . . . .	370
	v6rd . . . . .	371
<b>Chapter 10</b>	<b>Network Address Translation and Software Administration . . . . .</b>	<b>373</b>
	Monitoring Carrier-Grade NAT and Software . . . . .	373
	Monitoring CGN, Stateful Firewall, and Software Flows . . . . .	373
	Monitoring Stateful Firewall Conversations . . . . .	374
	Monitoring Global Stateful Firewall Statistics . . . . .	374
	Monitoring NAT Pool Usage . . . . .	375
	Monitoring Software Statistics . . . . .	375
	Ping and Traceroute for DS-Lite . . . . .	377
	Log Generation . . . . .	377
	Configuring NAT Session Logs . . . . .	378
	High Availability and Load Balancing for 6rd Softwares . . . . .	379
	Load Balancing a 6rd Domain Across Multiple Services PICs . . . . .	379
	Example: Load Balancing a 6rd Domain Across Multiple Services PICs . . . . .	379
	Configuring High Availability for 6rd Using 6rd Anycast . . . . .	384
	Protecting Against Denial of Service Attacks . . . . .	384
	Protecting CGN Devices Against Denial of Service (DOS) Attacks . . . . .	385
	Mapping Refresh Behavior . . . . .	385
	EIF Inbound Flow Limit . . . . .	385
<b>Chapter 11</b>	<b>Stateful Firewall Services Configuration Guidelines . . . . .</b>	<b>387</b>
	Configuring Stateful Firewall Rules . . . . .	388
	Configuring Match Direction for Stateful Firewall Rules . . . . .	388
	Configuring Match Conditions in Stateful Firewall Rules . . . . .	389
	Configuring Actions in Stateful Firewall Rules . . . . .	390
	Configuring IP Option Handling . . . . .	391
	Configuring Stateful Firewall Rule Sets . . . . .	392
	Examples: Configuring Stateful Firewall Rules . . . . .	392
<b>Chapter 12</b>	<b>Summary of Stateful Firewall Configuration Statements . . . . .</b>	<b>397</b>
	allow-ip-options . . . . .	398
	application-sets . . . . .	399
	applications . . . . .	399
	destination-address . . . . .	400
	destination-address-range . . . . .	400

	destination-prefix-list . . . . .	401
	from . . . . .	402
	match-direction . . . . .	402
	rule . . . . .	403
	rule-set . . . . .	404
	services (stateful-firewall) . . . . .	404
	source-address . . . . .	405
	source-address-range . . . . .	405
	source-prefix-list . . . . .	406
	syslog . . . . .	406
	term . . . . .	407
	then . . . . .	408
<b>Chapter 13</b>	<b>Stateful Firewall on the Embedded Junos OS Platform Configuration Guidelines . . . . .</b>	<b>409</b>
	Loading the Stateful Firewall Plug-In . . . . .	409
	Configuring Memory for the Stateful Firewall Plug-In . . . . .	411
	Configuring rsh, rlogin, rexec for Stateful Firewall . . . . .	411
<b>Chapter 14</b>	<b>Summary of Stateful Firewall on the Embedded Junos OS Platform Configuration Statements . . . . .</b>	<b>413</b>
	control-cores . . . . .	413
	data-cores . . . . .	414
	data-flow-affinity . . . . .	414
	destination (Chassis) . . . . .	415
	extension-provider . . . . .	416
	forwarding-db-size . . . . .	417
	hash-key (Chassis) . . . . .	418
	object-cache-size . . . . .	419
	package (Loading on PIC) . . . . .	420
	policy-db-size . . . . .	421
	syslog (Chassis) . . . . .	422
	wired-process-mem-size . . . . .	423
<b>Chapter 15</b>	<b>Load Balancing Configuration Guidelines . . . . .</b>	<b>425</b>
	Configuring Load Balancing on AMS Infrastructure . . . . .	425
	Configuring AMS Infrastructure . . . . .	426
	Configuring High Availability . . . . .	426
	Load Balancing Network Address Translation Flows . . . . .	427
	Example: Configuring Static Source Translation on AMS Infrastructure . . . . .	427
<b>Chapter 16</b>	<b>Summary of Load Balancing Configuration Statements . . . . .</b>	<b>431</b>
	drop-member-traffic (Aggregated Multiservices) . . . . .	432
	enable-rejoin (aggregated Multiservices) . . . . .	433
	family (aggregated Multiservices) . . . . .	433
	high-availability-options (aggregated Multiservices) . . . . .	434
	interfaces (Aggregated Multiservices) . . . . .	435
	load-balancing-options (Aggregated Multiservices) . . . . .	436
	many-to-one (Aggregated Multiservices) . . . . .	437
	member-failure-options (Aggregated Multiservices) . . . . .	438
	member-interface (Aggregated Multiservices) . . . . .	440

	redistribute-all-traffic (Aggregated Multiservices) . . . . .	441
	rejoin-timeout (Aggregated Multiservices) . . . . .	442
	unit (Aggregated Multiservices) . . . . .	443
<b>Chapter 17</b>	<b>Intrusion Detection Service Configuration Guidelines . . . . .</b>	<b>445</b>
	Configuring IDS Rules . . . . .	447
	Configuring Match Direction for IDS Rules . . . . .	448
	Configuring Match Conditions in IDS Rules . . . . .	449
	Configuring Actions in IDS Rules . . . . .	450
	Configuring IDS Rule Sets . . . . .	453
	Examples: Configuring IDS Rules . . . . .	454
<b>Chapter 18</b>	<b>Summary of Intrusion Detection Service Configuration Statements . . . .</b>	<b>457</b>
	aggregation . . . . .	457
	application-sets (Services IDS) . . . . .	458
	applications (Services IDS) . . . . .	458
	by-destination . . . . .	459
	by-pair . . . . .	460
	by-source . . . . .	461
	destination-address (Services IDS) . . . . .	462
	destination-address-range (Services IDS) . . . . .	462
	destination-prefix (Services IDS) . . . . .	463
	destination-prefix-ipv6 . . . . .	463
	destination-prefix-list (Services IDS) . . . . .	464
	force-entry . . . . .	464
	from (Services IDS) . . . . .	465
	ignore-entry . . . . .	465
	logging (Services IDS) . . . . .	466
	match-direction (Services IDS) . . . . .	466
	mss . . . . .	467
	rule (Services IDS) . . . . .	468
	rule-set (Services IDS) . . . . .	469
	services (IDS) . . . . .	469
	session-limit . . . . .	470
	source-address (Services IDS) . . . . .	471
	source-address-range (Services IDS) . . . . .	471
	source-prefix (Services IDS) . . . . .	472
	source-prefix-ipv6 . . . . .	472
	source-prefix-list (Services IDS) . . . . .	473
	syn-cookie . . . . .	473
	syslog (Services IDS) . . . . .	474
	term (Services IDS) . . . . .	475
	then (Services IDS) . . . . .	477
	threshold (Services) . . . . .	478

<b>Chapter 19</b>	<b>IPsec Services Configuration Guidelines</b>	<b>479</b>
	Minimum Security Association Configurations	481
	Minimum Manual SA Configuration	481
	Minimum Dynamic SA Configuration	482
	Configuring Security Associations	483
	Security Associations Overview	483
	Configuring Manual Security Associations	484
	Configuring the Direction for IPsec Processing	485
	Configuring the Protocol for a Manual IPsec SA	486
	Configuring the Security Parameter Index	486
	Configuring the Auxiliary Security Parameter Index	486
	Configuring Authentication for a Manual IPsec SA	486
	Configuring Encryption for a Manual IPsec SA	487
	Configuring Dynamic Security Associations	488
	Clearing Security Associations	489
	Configuring IKE Proposals	489
	Configuring the Authentication Algorithm for an IKE Proposal	490
	Configuring the Authentication Method for an IKE Proposal	491
	Configuring the Diffie-Hellman Group for an IKE Proposal	491
	Configuring the Encryption Algorithm for an IKE Proposal	492
	Configuring the Lifetime for an IKE SA	492
	Example: Configuring an IKE Proposal	493
	Configuring IKE Policies	493
	Configuring the IKE Phase	494
	Configuring the Mode for an IKE Policy	495
	Configuring the Proposals in an IKE Policy	495
	Configuring the Preshared Key for an IKE Policy	495
	Configuring the Local Certificate for an IKE Policy	496
	Configuring a Certificate Revocation List	496
	Configuring the Description for an IKE Policy	497
	Configuring Local and Remote IDs for IKE Phase 1 Negotiation	497
	Example: Configuring an IKE Policy	498
	Configuring IPsec Proposals	499
	Configuring the Authentication Algorithm for an IPsec Proposal	499
	Configuring the Description for an IPsec Proposal	499
	Configuring the Encryption Algorithm for an IPsec Proposal	500
	Configuring the Lifetime for an IPsec SA	500
	Configuring the Protocol for a Dynamic SA	501
	Configuring IPsec Policies	501
	Configuring the Description for an IPsec Policy	502
	Configuring Perfect Forward Secrecy	502
	Configuring the Proposals in an IPsec Policy	503
	Example: Configuring an IPsec Policy	503
	IPsec Policy for Dynamic Endpoints	504
	Configuring IPsec Rules	504
	Configuring Match Direction for IPsec Rules	505
	Configuring Match Conditions in IPsec Rules	506

Configuring Actions in IPsec Rules . . . . .	508
Enabling IPsec Packet Fragmentation . . . . .	509
Configuring Destination Addresses for Dead Peer Detection . . . . .	509
Configuring or Disabling IPsec Anti-Replay . . . . .	510
Enabling System Log Messages . . . . .	511
Specifying the MTU for IPsec Tunnels . . . . .	511
Configuring IPsec Rule Sets . . . . .	511
Configuring Dynamic Endpoints for IPsec Tunnels . . . . .	512
Authentication Process . . . . .	512
Implicit Dynamic Rules . . . . .	513
Reverse Route Insertion . . . . .	513
Configuring an IKE Access Profile . . . . .	514
Referencing the IKE Access Profile in a Service Set . . . . .	515
Configuring the Interface Identifier . . . . .	516
Default IKE and IPsec Proposals . . . . .	516
Tracing IPsec Operations . . . . .	517
Disabling IPsec Tunnel Endpoint in Traceroute . . . . .	518
Tracing IPsec PKI Operations . . . . .	518
Configuring IPsec Using the Extension-Provider Package . . . . .	519
Examples: Configuring IPsec Services . . . . .	520
Example: Configuring Statically Assigned Tunnels . . . . .	521
Example: Configuring Dynamically Assigned Tunnels . . . . .	524
Multitask Example: Configuring IPsec Services . . . . .	528
Configuring the IKE Proposal . . . . .	528
Configuring the IKE Policy (and Referencing the IKE Proposal) . . . . .	529
Configuring the IPsec Proposal . . . . .	529
Configuring the IPsec Policy (and Referencing the IPsec Proposal) . . . . .	530
Configuring the IPsec Rule (and Referencing the IKE and IPsec Policies) . . . . .	531
Configuring IPsec Trace Options . . . . .	532
Configuring the Access Profile (and Referencing the IKE and IPsec Policies) . . . . .	532
Configuring the Service Set (and Referencing the IKE Profile and the IPsec Rule) . . . . .	533
<b>Chapter 20 Summary of IPsec Services Configuration Statements . . . . .</b>	<b>535</b>
anti-replay-window-size (Services IPsec VPN) . . . . .	537
authentication (Services IPsec VPN) . . . . .	538
authentication-algorithm . . . . .	539
authentication-algorithm (Services IKE) . . . . .	539
authentication-algorithm (Services IPsec) . . . . .	540
authentication-method (Services IPsec VPN) . . . . .	540
auxiliary-spi (Services IPsec VPN) . . . . .	541
backup-remote-gateway . . . . .	541
clear-dont-fragment-bit (Services IPsec VPN) . . . . .	542
clear-ike-sas-on-pic-restart . . . . .	542
clear-ipsec-sas-on-pic-restart . . . . .	543
copy-dont-fragment-bit (Services IPsec VPN) . . . . .	543
description (Services IPsec VPN) . . . . .	544

destination-address (Services IPsec VPN) .....	544
dh-group .....	545
direction .....	546
dynamic .....	547
encryption .....	548
encryption-algorithm (Services IPsec VPN) .....	549
from (Services IPsec VPN) .....	550
ike .....	551
initiate-dead-peer-detection .....	552
ipsec (Services IPsec VPN) .....	553
ipsec-inside-interface .....	553
lifetime-seconds (Services IPsec VPN) .....	554
local-certificate (Services IPsec VPN) .....	554
local-id .....	555
manual .....	556
match-direction (Services IPsec VPN) .....	556
mode (Services IPsec VPN) .....	557
no-anti-replay (Services IPsec VPN) .....	557
no-ipsec-tunnel-in-traceroute .....	558
perfect-forward-secrecy (Services IPsec VPN) .....	558
policy .....	559
policy (Services IKE) .....	559
policy (Services IPsec VPN) .....	560
pre-shared-key (Services IKE) .....	560
proposal .....	561
proposal (Services IKE) .....	561
proposal (Services IPsec VPN) .....	562
proposals .....	562
protocol .....	563
remote-gateway .....	563
remote-id .....	564
rule (Services IPsec VPN) .....	565
rule-set (Services IPsec VPN) .....	566
services (IPsec VPN) .....	566
set-dont-fragment-bit (Services IPsec VPN) .....	567
source-address (Services IPsec VPN) .....	567
spi .....	568
syslog (Services IPsec VPN) .....	568
term (Services IPsec VPN) .....	569
then (Services IPsec VPN) .....	570
traceoptions (Services IPsec VPN) .....	571
traceoptions (PKI) .....	573
tunnel-mtu (Services IPsec VPN) .....	574
version (IKE) .....	575

<b>Chapter 21</b>	<b>Layer 2 Tunneling Protocol Services Configuration Guidelines . . . . .</b>	<b>577</b>
	L2TP Services Configuration Overview . . . . .	579
	L2TP Minimum Configuration . . . . .	580
	Configuring L2TP Tunnel Groups . . . . .	582
	Configuring Access Profiles for L2TP Tunnel Groups . . . . .	583
	Configuring the Local Gateway Address and PIC . . . . .	583
	Configuring Window Size for L2TP Tunnels . . . . .	584
	Configuring Timers for L2TP Tunnels . . . . .	584
	Hiding Attribute-Value Pairs for L2TP Tunnels . . . . .	585
	Configuring System Logging of L2TP Tunnel Activity . . . . .	585
	Configuring the Identifier for Logical Interfaces that Provide L2TP Services . . . . .	587
	Example: Configuring Multilink PPP on a Shared Logical Interface . . . . .	587
	AS PIC Redundancy for L2TP Services . . . . .	589
	IP Packet Fragment Reassembly for L2TP Overview . . . . .	589
	Configuring IP Inline Reassembly for L2TP . . . . .	590
	Tracing L2TP Operations . . . . .	591
	Examples: Configuring L2TP Services . . . . .	593
<b>Chapter 22</b>	<b>Summary of Layer 2 Tunneling Protocol Configuration Statements . . . . .</b>	<b>597</b>
	facility-override . . . . .	597
	hello-interval . . . . .	598
	hide-avps . . . . .	599
	host (L2TP) . . . . .	599
	ip-reassembly (L2TP) . . . . .	600
	l2tp-access-profile . . . . .	600
	local-gateway (L2TP LNS) . . . . .	601
	log-prefix (L2TP) . . . . .	601
	maximum-send-window . . . . .	602
	ppp-access-profile . . . . .	602
	receive-window . . . . .	603
	retransmit-interval (Services) . . . . .	603
	service-interface . . . . .	604
	services . . . . .	605
	services (Hierarchy) . . . . .	605
	services (L2TP System Logging) . . . . .	606
	syslog . . . . .	607
	traceoptions (L2TP) . . . . .	608
	tunnel-group . . . . .	612
	tunnel-timeout . . . . .	613
<b>Chapter 23</b>	<b>Link Services IQ Interfaces Configuration Guidelines . . . . .</b>	<b>615</b>
	Layer 2 Service Package Capabilities and Interfaces . . . . .	616
	Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET	
	APS . . . . .	618
	Configuring the Association between LSQ and SONET Interfaces . . . . .	618
	Configuring SONET APS Interoperability with Cisco Systems FRF.16 . . . . .	619
	Restrictions on APS Redundancy for LSQ Interfaces . . . . .	620
	Configuring LSQ Interface Redundancy in a Single Router Using SONET APS . . . . .	620

Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces . . . . .	621
Configuring Redundant Paired LSQ Interfaces . . . . .	621
Restrictions on Redundant LSQ Interfaces . . . . .	622
Configuring Link State Replication for Redundant Link PICs . . . . .	624
Examples: Configuring Redundant LSQ Interfaces for Failure Recovery . . .	625
Configuring CoS Scheduling Queues on Logical LSQ Interfaces . . . . .	630
Configuring Scheduler Buffer Size . . . . .	631
Configuring Scheduler Priority . . . . .	632
Configuring Scheduler Shaping Rate . . . . .	632
Configuring Drop Profiles . . . . .	632
Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces . . . . .	633
Reserving Bundle Bandwidth for Link-Layer Overhead on LSQ Interfaces . . . .	635
Configuring Multiclass MLPPP on LSQ Interfaces . . . . .	636
Oversubscribing Interface Bandwidth on LSQ Interfaces . . . . .	638
Examples: Oversubscribing an LSQ Interface . . . . .	641
Configuring Guaranteed Minimum Rate on LSQ Interfaces . . . . .	643
Example: Configuring Guaranteed Minimum Rate . . . . .	645
Configuring Link Services and CoS on Services PICs . . . . .	646
Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using MLPPP . . . . .	649
Example: Configuring an LSQ Interface as an NxT1 Bundle Using MLPPP . .	652
Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using FRF.16 . . . . .	655
Example: Configuring an LSQ Interface as an NxT1 Bundle Using FRF.16 . .	658
Configuring LSQ Interfaces for Single Fractional T1 or El Interfaces Using MLPPP and LFI . . . . .	660
Example: Configuring an LSQ Interface for a Fractional T1 Interface Using MLPPP and LFI . . . . .	663
Configuring LSQ Interfaces for Single Fractional T1 or El Interfaces Using FRF.12 . . . . .	665
Examples: Configuring an LSQ Interface for a Fractional T1 Interface Using FRF.12 . . . . .	668
Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using FRF.15 . . . . .	672
Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP . . . . .	673
Configuring LSQ Interfaces as T3 or OC3 Bundles Using FRF.12 . . . . .	675
Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP . . . . .	677
<b>Chapter 24 Summary of Link Services IQ Configuration Statements . . . . .</b>	<b>681</b>
cisco-interoperability . . . . .	681
forwarding-class . . . . .	682
fragment-threshold . . . . .	683
fragmentation-map . . . . .	683
fragmentation-maps . . . . .	684
hot-standby . . . . .	685
link-layer-overhead . . . . .	685
lsq-failure-options . . . . .	686
multilink-class . . . . .	686
multilink-max-classes . . . . .	687
no-fragmentation . . . . .	688

	no-per-unit-scheduler . . . . .	688
	no-termination-request . . . . .	689
	per-unit-scheduler . . . . .	690
	preserve-interface . . . . .	691
	primary . . . . .	691
	redundancy-options . . . . .	692
	secondary . . . . .	692
	trigger-link-failure . . . . .	693
	warm-standby . . . . .	693
<b>Chapter 25</b>	<b>Voice Services Configuration Guidelines . . . . .</b>	<b>695</b>
	Configuring Services Interfaces for Voice Services . . . . .	696
	Configuring the Logical Interface Address for the MLPPP Bundle . . . . .	696
	Configuring Compression of Voice Traffic . . . . .	697
	Configuring Delay-Sensitive Packet Interleaving . . . . .	698
	Example: Configuring Compression of Voice Traffic . . . . .	698
	Configuring Encapsulation for Voice Services . . . . .	699
	Configuring Network Interfaces for Voice Services . . . . .	700
	Configuring Voice Services Bundles with MLPPP Encapsulation . . . . .	700
	Configuring the Compression Interface with PPP Encapsulation . . . . .	700
	Examples: Configuring Voice Services . . . . .	701
<b>Chapter 26</b>	<b>Summary of Voice Services Configuration Statements . . . . .</b>	<b>705</b>
	address (Interfaces) . . . . .	706
	bundle . . . . .	706
	compression . . . . .	707
	compression-device (Interfaces) . . . . .	707
	encapsulation . . . . .	708
	f-max-period . . . . .	708
	family (Interfaces) . . . . .	709
	fragment-threshold (Interfaces LSQ) . . . . .	710
	interfaces . . . . .	710
	maximum-contexts . . . . .	711
	port . . . . .	712
	queues . . . . .	712
	rtp . . . . .	713
	unit (Interfaces) . . . . .	714
<b>Chapter 27</b>	<b>Class-of-Service Configuration Guidelines . . . . .</b>	<b>715</b>
	Restrictions and Cautions for CoS Configuration on Services Interfaces . . . . .	716
	Configuring CoS Rules . . . . .	717
	Configuring Match Direction for CoS Rules . . . . .	718
	Configuring Match Conditions In CoS Rules . . . . .	718
	Configuring Actions in CoS Rules . . . . .	719
	Configuring Application Profiles for Use as CoS Rule Actions . . . . .	720
	Configuring Reflexive and Reverse CoS Rule Actions . . . . .	721
	Example: Configuring CoS Rules . . . . .	721
	Configuring CoS Rule Sets . . . . .	722
	Examples: Configuring CoS on Services Interfaces . . . . .	722

<b>Chapter 28</b>	<b>Summary of Class-of-Service Configuration Statements . . . . .</b>	<b>725</b>
	application-profile . . . . .	726
	application-sets (Services CoS) . . . . .	727
	applications (Services CoS) . . . . .	727
	data (FTP) . . . . .	728
	destination-address (CoS) . . . . .	728
	destination-prefix-list (Services CoS) . . . . .	729
	dscp . . . . .	729
	forwarding-class . . . . .	730
	from (Services CoS) . . . . .	730
	ftp (Class-Of-Service) . . . . .	731
	match-direction . . . . .	731
	(reflexive   reverse) . . . . .	732
	rule . . . . .	733
	rule-set (Services CoS) . . . . .	734
	services (COS) . . . . .	734
	sip (Application Profile) . . . . .	735
	source-address (Services CoS) . . . . .	735
	source-prefix-list . . . . .	736
	syslog (Services CoS) . . . . .	736
	term (Services CoS) . . . . .	737
	then . . . . .	738
	video (Application Profile) . . . . .	738
	voice (Application Profile) . . . . .	739
<b>Chapter 29</b>	<b>Service Set Configuration Guidelines . . . . .</b>	<b>741</b>
	Configuring Service Sets to be Applied to Services Interfaces . . . . .	742
	Configuring Interface Service Sets . . . . .	742
	Configuring Next-Hop Service Sets . . . . .	744
	Determining Traffic Direction . . . . .	745
	Interface Style Service Sets . . . . .	746
	Next-Hop Style Service Sets . . . . .	746
	Configuring Service Rules . . . . .	747
	Configuring IPsec Service Sets . . . . .	748
	Configuring the Local Gateway Address for IPsec Service Sets . . . . .	748
	IKE Addresses in VRF Instances . . . . .	749
	Configuring IKE Access Profiles for IPsec Service Sets . . . . .	750
	Configuring Certification Authorities for IPsec Service Sets . . . . .	750
	Configuring or Disabling Antireplay Service . . . . .	750
	Clearing the Don't-Fragment Bit . . . . .	751
	Configuring Passive-Mode Tunneling . . . . .	752
	Configuring the Tunnel MTU Value . . . . .	752
	Configuring Service Set Limitations . . . . .	753
	Configuring System Logging for Service Sets . . . . .	754
	Enabling Services PICs to Accept Multicast Traffic . . . . .	756
	Tracing Services PIC Operations . . . . .	756
	Configuring the Adaptive Services Log Filename . . . . .	757
	Configuring the Number and Size of Adaptive Services Log Files . . . . .	757
	Configuring Access to the Log File . . . . .	758

	Configuring a Regular Expression for Lines to Be Logged . . . . .	758
	Configuring the Trace Operations . . . . .	758
	Example: Configuring Service Sets . . . . .	759
<b>Chapter 30</b>	<b>Summary of Service Set Configuration Statements . . . . .</b>	<b>761</b>
	adaptive-services-pics . . . . .	762
	allow-multicast . . . . .	763
	anti-replay-window-size (Services Service Set) . . . . .	764
	bypass-traffic-on-exceeding-flow-limits . . . . .	765
	bypass-traffic-on-pic-failure . . . . .	765
	clear-dont-fragment-bit (Services Service Set) . . . . .	766
	copy-dont-fragment-bit (Services Set) . . . . .	767
	facility-override . . . . .	768
	host (service-set) . . . . .	769
	ids-rules . . . . .	770
	ike-access-profile . . . . .	770
	interface-service . . . . .	771
	ip-reassembly-rules (Service Set) . . . . .	771
	ipsec-vpn-options . . . . .	772
	ipsec-vpn-rules . . . . .	772
	local-gateway . . . . .	773
	log-prefix (Services) . . . . .	773
	logging (Services) . . . . .	774
	max-flows . . . . .	775
	message-rate-limit . . . . .	776
	nat-options . . . . .	777
	nat-rules . . . . .	777
	next-hop-service . . . . .	778
	no-anti-replay (Services Service Set) . . . . .	779
	passive-mode-tunneling . . . . .	780
	pgcp-rules . . . . .	780
	port (syslog) . . . . .	781
	ptsp-rules . . . . .	781
	service-interface . . . . .	782
	service-set (Services) . . . . .	783
	service-set-options . . . . .	785
	software-options . . . . .	785
	services . . . . .	786
	services (Hierarchy) . . . . .	786
	services (System Logging) . . . . .	787
	set-dont-fragment-bit (Services Set) . . . . .	788
	stateful-firewall-rules . . . . .	788
	syslog (Services Service Set) . . . . .	789
	tcp-mss . . . . .	790
	traceoptions (Services Logging) . . . . .	791
	trusted-ca . . . . .	792
	tunnel-mtu (Services Service Set) . . . . .	793

<b>Chapter 31</b>	<b>Service Interface Configuration Guidelines . . . . .</b>	<b>795</b>
	Services Interface Naming Overview . . . . .	797
	Configuring the Address and Domain for Services Interfaces . . . . .	798
	Configuring Default Timeout Settings for Services Interfaces . . . . .	799
	Configuring System Logging for Services Interfaces . . . . .	801
	Enabling Fragmentation on GRE Tunnels . . . . .	802
	Applying Filters and Services to Interfaces . . . . .	803
	Configuring Service Filters . . . . .	804
	Configuring AS or Multiservices PIC Redundancy . . . . .	806
	Flow Offloading . . . . .	808
	Configuring Fragmentation Control for MS-DPC and MS-PIC Service Interfaces. . . . .	809
	Examples: Configuring Services Interfaces . . . . .	809
<b>Chapter 32</b>	<b>Summary of Service Interface Configuration Statements . . . . .</b>	<b>813</b>
	address (Interfaces) . . . . .	814
	cgn-pic . . . . .	815
	clear-dont-fragment-bit . . . . .	815
	close-timeout . . . . .	816
	dial-options . . . . .	817
	facility-override . . . . .	818
	family (Interfaces) . . . . .	819
	host (Interfaces) . . . . .	820
	hot-standby . . . . .	820
	inactivity-timeout . . . . .	821
	input (Interfaces) . . . . .	821
	interfaces . . . . .	822
	log-prefix (Interfaces) . . . . .	822
	maximum . . . . .	823
	open-timeout . . . . .	823
	output . . . . .	824
	post-service-filter . . . . .	824
	primary (Interfaces) . . . . .	825
	rate . . . . .	825
	redundancy-options . . . . .	826
	secondary (Interfaces) . . . . .	826
	service . . . . .	827
	service-domain . . . . .	828
	service-filter (Interfaces) . . . . .	828
	service-set (Interfaces) . . . . .	829
	services (Interfaces) . . . . .	830
	services-options . . . . .	831
	session-limit . . . . .	832
	source-address . . . . .	832
	syslog (Interfaces) . . . . .	833
	tcp-tickles . . . . .	833
	trio-flow-offload . . . . .	834
	unit . . . . .	835

<b>Chapter 33</b>	<b>PGCP Configuration Guidelines for the BGF Feature</b>	<b>837</b>
<b>Chapter 34</b>	<b>Summary of PGCP Configuration Statements</b>	<b>843</b>
	administrative	847
	administrative (Control Association)	847
	administrative (Virtual Interface)	848
	algorithm	849
	application-data-inactivity-detection	849
	audit-observed-events-returns	850
	base-root	851
	bgf-core	852
	cancel-graceful	854
	cancel-graceful (Control Association)	854
	cancel-graceful (Virtual Interface)	855
	cleanup-timeout	855
	context-indications	856
	control-association-indications	857
	controller-address	858
	controller-failure	858
	controller-port	859
	data-inactivity-detection (Services PGCP)	859
	default	860
	delivery-function	861
	destination-address	861
	destination-port	862
	detect	862
	diffserv	863
	disable-session-mirroring	863
	disconnect	864
	down	865
	dscp (Services PGCP)	866
	encoding	866
	event-timestamp-notification	867
	failover-cold	867
	failover-warm	868
	failure	869
	fast-update-filters	870
	file (Services PGCP)	871
	flag (Services PGCP)	872
	gateway (Services PGCP)	873
	gateway-address	877
	gateway-controller	878
	gateway-port	879
	graceful	880
	graceful (Control Association)	880
	graceful (Virtual Interface)	881
	graceful-restart	881
	h248-options	882
	h248-profile	884

h248-properties	885
h248-stack	888
h248-timers	889
hanging-termination-detection	889
inactivity-delay	890
inactivity-duration (Services PGCP)	890
inactivity-timeout	891
inactivity-timer	892
initial-average-ack-delay	892
interim-ah-scheme	893
ip-flow-stop-detection	893
ipsec-transport-security-association	894
latch-deadlock-delay	894
max-burst-size	895
max-burst-size (All Streams)	895
max-burst-size (RTCP Streams)	896
max-concurrent-calls	897
maximum-fuf-percentage	898
maximum-inactivity-time	899
maximum-net-propagation-delay	900
maximum-synchronization-mismatches	900
maximum-terms	901
maximum-waiting-delay	901
media	902
mg-maximum-pdu-size	903
mg-originated-pending-limit	904
mg-provisional-response-timer-value	905
mg-segmentation-timer	906
mgc-maximum-pdu-size	907
mgc-originated-pending-limit	908
mgc-provisional-response-timer-value	909
mgc-segmentation-timer	910
monitor	911
network-operator-id	911
no-dscp-bit-mirroring	912
no-rtcp-check	912
normal-mg-execution-time	913
normal-mgc-execution-time	914
notification-behavior	915
notification-rate-limit	915
notification-regulation	916
overload-control	916
peak-data-rate	917
peak-data-rate (All Streams)	917
peak-data-rate (RTCP)	918
platform	919
profile-name	920
profile-version	920
queue-limit-percentage	921

	reconnect	922
	reject-all-commands-threshold	922
	reject-new-calls-threshold	923
	report-service-change	923
	request-timestamp	924
	routing-instance	924
	rtcp	925
	rtp	925
	rule	926
	rule-set	926
	sbc-utils (Services PGCP)	927
	segmentation	928
	send-notification-on-delay	929
	service-change	930
	service-change-type	931
	service-interface	931
	service-state	932
	service-state (Virtual BGF)	932
	service-state (Virtual Interface)	933
	services (PGCP)	933
	session-mirroring	934
	source-address	934
	source-port (Mirrored BGF Packets)	935
	state-loss	936
	stop-detection-on-drop	936
	sustained-data-rate	937
	sustained-data-rate (All Streams)	937
	sustained-data-rate (RTCP Streams)	938
	timerx	939
	tmax-retransmission-delay	939
	traceoptions (Services PGCP)	940
	traffic-management	941
	up	942
	use-lower-case	942
	use-wildcard-response	943
	virtual-interface	944
	virtual-interface-down	945
	virtual-interface-indications	946
	virtual-interface-up	946
	warm	947
<b>Chapter 35</b>	<b>Service Interface Pools Configuration Guidelines</b>	<b>949</b>
	Configuring Service Interface Pools	949
<b>Chapter 36</b>	<b>Summary of Service Interface Pools Statements</b>	<b>951</b>
	interface	951
	pool	952
	service-interface-pools	952

<b>Chapter 37</b>	<b>PTSP Configuration Guidelines . . . . .</b>	<b>953</b>
<b>Chapter 38</b>	<b>Summary of PTSP Configuration Statements . . . . .</b>	<b>955</b>
	application-group-any . . . . .	956
	application-groups . . . . .	956
	applications (Services PTSP) . . . . .	957
	count-type . . . . .	957
	demux . . . . .	958
	forward-rule (Configuring) . . . . .	959
	forward-rule (Including in Rule) . . . . .	960
	from (Forward Rule) . . . . .	960
	from (Rule) . . . . .	961
	local-address . . . . .	962
	local-address-range . . . . .	963
	local-port-range . . . . .	963
	local-ports . . . . .	964
	local-prefix-list . . . . .	964
	match-direction (Services PTSP) . . . . .	965
	protocol . . . . .	965
	remote-address . . . . .	966
	remote-address-range . . . . .	967
	remote-port-range . . . . .	967
	remote-ports . . . . .	968
	remote-prefix-list . . . . .	968
	rule (Configuring) . . . . .	969
	rule (Including in Rule Set) . . . . .	970
	rule-set (Services PTSP) . . . . .	970
	services (PTSP) . . . . .	971
	term (Forward Rule) . . . . .	972
	term (Rule) . . . . .	973
	then (Forward Rule) . . . . .	974
	then (Rule) . . . . .	975
<b>Part 3</b>	<b>Junos Application Aware</b>	
<b>Chapter 39</b>	<b>Junos Application Aware Overview . . . . .</b>	<b>979</b>
	IDP Overview . . . . .	980
	APPID Overview . . . . .	982
	AACL Overview . . . . .	984
	L-PDF Overview . . . . .	986
	Configuring Multiple IDP Detectors . . . . .	988
	Best-Effort Application Identification of DPI-Serviced Flows . . . . .	988
	Features that Support Application-Level Filtering . . . . .	988
	Best-Effort Application Determination . . . . .	989
	APPID, AACL, and L-PDF Processing in Preconvergence Scenarios . . . . .	989
	Prior to a Final or Best-Effort Application Identification . . . . .	989
	Upon Best-Effort Application Identification . . . . .	989
	While Application Identification Is on a Best-Effort Basis . . . . .	990
	If a Flow Ends Before an Application Identification Is Made . . . . .	990

	If a Flow Ends While Application Identification on a Best-Effort Basis . . . . .	990
<b>Chapter 40</b>	<b>Application Identification Configuration Guidelines . . . . .</b>	<b>993</b>
	Defining an Application Identification . . . . .	995
	Configuring APPID Rules . . . . .	997
	Using Stateful Firewall Rules to Identify Data Sessions . . . . .	999
	Configuring Application Profiles . . . . .	1001
	Configuring Application Groups . . . . .	1001
	Application Identification for Nested Applications . . . . .	1002
	Disabling Application Identification for Nested Applications . . . . .	1004
	Configuring Global APPID Properties . . . . .	1004
	Configuring Automatic Download of Application Package Updates . . . . .	1005
	Configuring APPID Support for Heuristics . . . . .	1006
	Configuring APPID Support for Unidirectional Traffic . . . . .	1007
	Tracing APPID Operations . . . . .	1008
	Configuring the APPID Log Filename . . . . .	1008
	Configuring the Number and Size of APPID Log Files . . . . .	1009
	Configuring Access to the Log File . . . . .	1009
	Configuring a Regular Expression for Lines to Be Logged . . . . .	1009
	Configuring the Tracing Flags . . . . .	1009
	Examples: Configuring Application Identification Properties . . . . .	1010
<b>Chapter 41</b>	<b>Summary of Application Identification Configuration Statements . . . . .</b>	<b>1013</b>
	address . . . . .	1015
	application . . . . .	1016
	application (Defining) . . . . .	1016
	application (Including in Rule) . . . . .	1017
	application-group . . . . .	1017
	application-groups (Services Application Identification) . . . . .	1018
	application-system-cache-timeout . . . . .	1018
	applications (Services Application Identification) . . . . .	1019
	automatic . . . . .	1019
	bypass-traffic-on-pic-failure . . . . .	1020
	chain-order . . . . .	1020
	context . . . . .	1021
	destination (Services) . . . . .	1021
	direction . . . . .	1022
	disable . . . . .	1023
	disable (APPID Application) . . . . .	1023
	disable (APPID Application Group) . . . . .	1023
	disable (APPID Port Mapping) . . . . .	1024
	disable-global-timeout-override . . . . .	1024
	download . . . . .	1025
	enable-heuristics . . . . .	1025
	enable-asymmetric-traffic-processing . . . . .	1026
	enable-heuristics . . . . .	1026
	idle-timeout . . . . .	1027
	ignore-errors . . . . .	1027
	inactivity-non-tcp-timeout . . . . .	1028

inactivity-tcp-timeout	1028
index (Nested Applications)	1029
index	1029
ip	1030
max-checked-bytes	1030
maximum-transactions	1031
member	1031
min-checked-bytes	1032
nested-application	1033
nested-application-settings	1034
no-application-identification	1034
no-application-system-cache	1035
no-clear-application-system-cache	1035
no-nested-application	1036
no-protocol-method	1036
no-signature-based	1037
order (Services Application Identification)	1037
pattern	1038
port-mapping	1038
port-range	1039
profile	1039
protocol	1040
hcm	1041
from	1041
host	1042
request-url	1042
term	1043
then	1043
url	1044
url-list	1044
url-rule	1045
url-rule-set	1045
rule	1046
rule (Configuring)	1046
rule (Including in Rule Set)	1047
rule-set (Services Application Identification)	1047
service-set (Services)	1048
service-set-options	1050
services (Application Identification)	1050
session-timeout	1051
session-timeout (Interfaces)	1051
session-timeout (Application Identification)	1051
signature	1052
signature-method-all-ports	1052
source	1053
support-uni-directional-traffic	1053
traceoptions (Application Identification)	1054
type	1055
type-of-service	1055

	url .....	1056
<b>Chapter 42</b>	<b>Application-Aware Access List Configuration Guidelines .....</b>	<b>1057</b>
	Configuring AACL Rules .....	1058
	Configuring Match Direction for AACL Rules .....	1059
	Configuring Match Conditions in AACL Rules .....	1059
	Configuring Actions in AACL Rules .....	1060
	Logging AACL Flows Based on Application .....	1061
	Configuring AACL Rule Sets .....	1062
	Configuring Logging of AACL Flows .....	1063
	Example: Configuring AACL Rules .....	1064
<b>Chapter 43</b>	<b>Summary of AACL Configuration Statements .....</b>	<b>1067</b>
	applications (Services AACL) .....	1067
	application-groups (Services AACL) .....	1068
	application-group-any .....	1068
	application-unknown .....	1068
	destination-address .....	1069
	destination-address-range .....	1069
	destination-prefix-list .....	1070
	from .....	1070
	match-direction .....	1071
	rule .....	1072
	rule-set (Services AACL) .....	1073
	services (AACL) .....	1073
	source-address (AACL) .....	1074
	source-address-range .....	1074
	source-prefix-list .....	1075
	term .....	1076
	then .....	1077
<b>Chapter 44</b>	<b>Local Policy Decision Function Configuration Guidelines .....</b>	<b>1079</b>
	Configuring Statistics Profiles .....	1079
	Configuring an L-PDF Statistics Profile .....	1080
	Configuring an AACL Statistics Profile .....	1081
	Applying L-PDF Profiles to Service Sets .....	1083
	Tracing L-PDF Operations .....	1084
<b>Chapter 45</b>	<b>Summary of L-PDF Configuration Statements .....</b>	<b>1087</b>
	aac-fields .....	1088
	aac-statistics-profile .....	1089
	application-aware-access-list-fields .....	1090
	file .....	1091
	local-policy-decision-function .....	1092
	policy-decision-statistics-profile .....	1093
	statistics (System Services) .....	1094
	traceoptions (Services Local Policy Decision Function) .....	1095

<b>Part 4</b>	<b>Encryption Services</b>	
<b>Chapter 46</b>	<b>Encryption Overview</b>	<b>1099</b>
	Encryption Overview	1099
<b>Chapter 47</b>	<b>Encryption Interfaces Configuration Guidelines</b>	<b>1101</b>
	Configuring Encryption Interfaces	1101
	Specifying the Security Association Name for Encryption Interfaces	1102
	Configuring the MTU for Encryption Interfaces	1102
	Example: Configuring an Encryption Interface	1102
	Configuring Filters for Traffic Transiting the ES PIC	1103
	Traffic Overview	1103
	Configuring the Security Association	1104
	Configuring an Outbound Traffic Filter	1105
	Example: Configuring an Outbound Traffic Filter	1105
	Applying the Outbound Traffic Filter	1106
	Example: Applying the Outbound Traffic Filter	1106
	Configuring an Inbound Traffic Filter	1106
	Example: Configuring an Inbound Traffic Filter	1107
	Applying the Inbound Traffic Filter to the Encryption Interface	1107
	Example: Applying the Inbound Traffic Filter to the Encryption Interface	1107
	Configuring an ES Tunnel Interface for a Layer 3 VPN	1108
	Configuring ES PIC Redundancy	1109
	Example: Configuring ES PIC Redundancy	1109
	Configuring IPsec Tunnel Redundancy	1110
<b>Chapter 48</b>	<b>Summary of Encryption Configuration Statements</b>	<b>1111</b>
	address (Interfaces)	1111
	backup-destination	1111
	backup-interface	1112
	destination (Interfaces)	1113
	es-options	1114
	family	1115
	filter	1116
	interfaces	1116
	ipsec-sa	1117
	source	1117
	tunnel	1118
	unit (Interfaces)	1119
<b>Part 5</b>	<b>Flow Monitoring and Discard Accounting Services</b>	
<b>Chapter 49</b>	<b>Flow Monitoring and Discard Accounting Overview</b>	<b>1123</b>
	Passive Flow Monitoring Overview	1124
	Active Flow Monitoring Overview	1125
<b>Chapter 50</b>	<b>Flow Monitoring and Discard Accounting Configuration Guidelines</b>	<b>1129</b>
	Configuring Traffic Sampling	1134
	Configuring Firewall Filter for Traffic Sampling	1135
	Configuring Traffic Sampling on a Logical Interface	1136

Disabling Traffic Sampling . . . . .	1137
Sampling Once . . . . .	1137
Preserving Prerewrite ToS Value for Egress Sampled or Mirrored Packets . . . . .	1137
Configuring Traffic Sampling Output . . . . .	1138
Traffic Sampling Output Format . . . . .	1140
Tracing Traffic Sampling Operations . . . . .	1140
Traffic Sampling Examples . . . . .	1141
Example: Sampling a Single SONET/SDH Interface . . . . .	1141
Example: Sampling All Traffic from a Single IP Address . . . . .	1142
Example: Sampling All FTP Traffic . . . . .	1143
Configuring Flow Monitoring . . . . .	1144
Configuring Flow-Monitoring Interfaces . . . . .	1144
Configuring Flow-Monitoring Properties . . . . .	1145
Directing Traffic to Flow-Monitoring Interfaces . . . . .	1146
Exporting Flows . . . . .	1146
Configuring Time Periods when Flow Monitoring is Active and Inactive . . . . .	1147
Example: Configuring Flow Monitoring . . . . .	1147
Example: Configuring Active Monitoring on Logical Systems . . . . .	1148
Enabling Flow Aggregation . . . . .	1151
Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd . . . . .	1152
Configuring Flow Aggregation to Use Version 9 Flow Templates . . . . .	1156
Configuring the Traffic to Be Sampled . . . . .	1157
Configuring the Version 9 Template Properties . . . . .	1157
Customizing Template ID, Observation Domain ID, and Source ID for Version 9 flow Templates . . . . .	1159
Restrictions . . . . .	1159
Fields Included in Each Template Type . . . . .	1160
MPLS Sampling Behavior . . . . .	1161
Verification . . . . .	1162
Examples: Configuring Version 9 Flow Templates . . . . .	1162
Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows . . . . .	1167
Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows . . . . .	1172
Sampling Instance Configuration . . . . .	1175
Configuring Inline Sampling . . . . .	1176
Configuring Inline Sampling on MX80 Routers . . . . .	1181
Directing Replicated Flows to Multiple Flow Servers . . . . .	1182
Directing Replicated Routing Engine–Based Sampling Flows to Multiple Servers . . . . .	1183
Directing Replicated Version 9 Flow Aggregates to Multiple Servers . . . . .	1184
Logging cflowd Flows Before Export . . . . .	1185
Configuring Port Mirroring . . . . .	1186
Configuring Tunnels . . . . .	1187
Port Mirroring with Next-Hop Groups . . . . .	1188
Configuring Inline Port Mirroring . . . . .	1189
Filter-Based Forwarding with Multiple Monitoring Interfaces . . . . .	1190

	Restrictions .....	1190
	Configuring Port Mirroring on Services Interfaces .....	1191
	Examples: Configuring Port Mirroring .....	1192
	Load Balancing Among Multiple Monitoring Interfaces .....	1199
	Configuring Discard Accounting .....	1202
	Enabling Passive Flow Monitoring .....	1203
	Passive Flow Monitoring for MPLS Encapsulated Packets .....	1205
	Removing MPLS Labels from Incoming Packets .....	1205
	Example: Enabling IPv4 Passive Flow Monitoring .....	1206
	Example: Enabling IPv6 Passive Flow Monitoring .....	1208
	Configuring Services Interface Redundancy with Flow Monitoring .....	1210
<b>Chapter 51</b>	<b>Summary of Flow-Monitoring Configuration Statements .....</b>	<b>1213</b>
	accounting .....	1216
	address (Interfaces) .....	1217
	aggregate-export-interval .....	1217
	aggregation .....	1218
	autonomous-system-type .....	1219
	cflowd .....	1220
	cflowd (Discard Accounting) .....	1220
	cflowd (Flow Monitoring) .....	1221
	core-dump .....	1222
	destination (Tunnel Remote End) .....	1223
	disable (Forwarding Options) .....	1223
	disable-all-instances .....	1224
	engine-id (Forwarding Options) .....	1224
	engine-type .....	1225
	extension-service .....	1226
	export-format .....	1227
	family .....	1228
	family (Interfaces) .....	1228
	family (Monitoring) .....	1229
	family (Port Mirroring) .....	1230
	family (Sampling) .....	1231
	file .....	1233
	file (Sampling) .....	1233
	file (Trace Options) .....	1234
	filename .....	1234
	files .....	1235
	filter .....	1236
	flow-active-timeout .....	1237
	flow-export-rate .....	1238
	flow-control-options .....	1238
	flow-export-destination .....	1239
	flow-inactive-timeout .....	1240
	flow-monitoring .....	1241
	flow-server .....	1242
	forwarding-options .....	1243
	inline-jflow .....	1243

input	1244
input (Port Mirroring)	1244
input (Sampling)	1245
input-interface-index	1245
instance	1246
instance (Port Mirroring)	1246
instance (Sampling)	1247
interface	1249
interface (Accounting or Sampling)	1249
interface (Monitoring)	1250
interface (Port Mirroring)	1250
interfaces	1251
ipv4-template	1251
ipv6-template	1252
label-position	1252
local-dump	1253
match	1253
maximum-packet-length	1254
max-packets-per-second	1255
monitoring	1256
mpls-ipv4-template	1257
mpls-template	1257
multiservice-options	1258
next-hop (Forwarding Options)	1258
next-hop-group	1259
next-hop-group (Forwarding Options)	1259
next-hop-group (Port Mirroring)	1260
no-core-dump	1260
no-filter-check	1260
no-local-dump	1260
no-remote-trace (Trace Options)	1261
no-stamp	1261
no-syslog	1261
no-world-readable	1261
observation-domain-id	1262
option-refresh-rate	1263
options-template-id	1264
output	1265
output (Accounting)	1265
output (Monitoring)	1266
output (Port Mirroring)	1267
output (Sampling)	1268
output-interface-index	1269
passive-monitor-mode	1270
pop-all-labels	1271
port	1272
port-mirroring	1273
rate (Forwarding Options)	1274
receive-options-packets	1274

	receive-ttl-exceeded . . . . .	1275
	required-depth . . . . .	1275
	run-length . . . . .	1276
	sample-once . . . . .	1276
	sampling . . . . .	1277
	sampling (Forwarding Options) . . . . .	1278
	sampling (Interfaces) . . . . .	1280
	services . . . . .	1281
	size . . . . .	1281
	source-address (Forwarding Options) . . . . .	1282
	source-id . . . . .	1282
	stamp . . . . .	1283
	syslog . . . . .	1283
	template . . . . .	1284
	template (Forwarding Options) . . . . .	1284
	template (Services) . . . . .	1285
	template-id . . . . .	1286
	template-refresh-rate . . . . .	1287
	traceoptions (Forwarding Options) . . . . .	1287
	unit . . . . .	1288
	version . . . . .	1289
	version9 . . . . .	1290
	version9 (Forwarding Options) . . . . .	1290
	version9 (Services) . . . . .	1291
	version-ipfix . . . . .	1292
	version-ipfix (Forwarding Options) . . . . .	1292
	version-ipfix (Services) . . . . .	1293
	world-readable . . . . .	1293
<b>Chapter 52</b>	<b>Flow Collection Configuration Guidelines . . . . .</b>	<b>1295</b>
	Configuring Flow Collection . . . . .	1297
	Configuring Destination FTP Servers for Flow Records . . . . .	1297
	Configuring a Packet Analyzer . . . . .	1297
	Configuring File Formats . . . . .	1298
	Configuring Interface Mappings . . . . .	1298
	Configuring Transfer Logs . . . . .	1299
	Configuring Retry Attempts . . . . .	1299
	Sending cflowd Records to Flow Collector Interfaces . . . . .	1300
	Configuring Flow Collection Mode and Interfaces on Services PICs . . . . .	1300
	Example: Configuring Flow Collection . . . . .	1301
<b>Chapter 53</b>	<b>Summary of Flow Collection Configuration Statements . . . . .</b>	<b>1309</b>
	analyzer-address . . . . .	1309
	analyzer-id . . . . .	1310
	archive-sites . . . . .	1310
	collector . . . . .	1311
	data-format . . . . .	1311
	destinations . . . . .	1312

	filename-prefix .....	1312
	file-specification .....	1313
	file-specification (File Format) .....	1313
	file-specification (Interface Mapping) .....	1313
	flow-collector .....	1314
	ftp .....	1316
	ftp (Flow Collector Files) .....	1317
	ftp (Transfer Log Files) .....	1318
	interface-map .....	1318
	maximum-age .....	1319
	name-format .....	1320
	password .....	1322
	password (Flow Collector File Servers) .....	1322
	password (Transfer Log File Servers) .....	1322
	retry (Services Flow Collector) .....	1323
	retry-delay .....	1323
	transfer .....	1324
	transfer-log-archive .....	1324
	username (Services) .....	1325
	variant .....	1325
<b>Chapter 54</b>	<b>Dynamic Flow Capture Configuration Guidelines .....</b>	<b>1327</b>
	Understanding Junos Capture Vision .....	1327
	Junos Capture Vision Architecture .....	1327
	Liberal Sequence Windowing .....	1328
	Intercepting IPv6 Flows .....	1329
	Configuring Junos Capture Vision .....	1329
	Configuring the Capture Group .....	1329
	Configuring the Content Destination .....	1330
	Configuring the Control Source .....	1331
	Configuring the DFC PIC Interface .....	1332
	Configuring the Firewall Filter .....	1333
	Configuring System Logging .....	1333
	Configuring Tracing Options for Junos Capture Vision Events .....	1334
	Configuring Thresholds .....	1334
	Limiting the Number of Duplicates of a Packet .....	1335
	Example: Configuring Junos Capture Vision .....	1335
<b>Chapter 55</b>	<b>Flow-Tap Configuration Guidelines .....</b>	<b>1339</b>
	Junos Packet Vision Architecture .....	1340
	Configuring Junos Packet Vision .....	1342
	Configuring the Junos Packet Vision Interface .....	1342
	Strengthening Junos Packet Vision Security .....	1342
	Restrictions on Junos Packet Vision Services .....	1343
	Configuring FlowTapLite .....	1344
	Examples: Configuring Junos Packet Vision .....	1346

<b>Chapter 56</b>	<b>Summary of Dynamic Flow Capture and Flow-Tap Configuration</b>	
	<b>Statements</b>	<b>1349</b>
	address (Services Dynamic Flow Capture)	1349
	allowed-destinations	1350
	capture-group	1351
	content-destination	1352
	control-source	1353
	duplicates-dropped-periodicity	1354
	dynamic-flow-capture	1355
	flow-tap	1356
	g-duplicates-dropped-periodicity	1357
	g-max-duplicates	1358
	hard-limit	1358
	hard-limit-target	1359
	input-packet-rate-threshold	1359
	interface (Services Flow Tap)	1360
	interfaces (Services Dynamic Flow Capture)	1360
	max-duplicates	1361
	minimum-priority	1361
	no-syslog	1362
	notification-targets	1362
	pic-memory-threshold	1363
	service-port	1363
	services (Dynamic Flow Capture)	1364
	shared-key	1364
	soft-limit	1365
	soft-limit-clear	1365
	source-addresses	1366
	traceoptions (Dynamic Flow Capture)	1367
	ttl	1368
<b>Part 6</b>	<b>Link and Multilink Services</b>	
<b>Chapter 57</b>	<b>Link and Multilink Services Overview</b>	<b>1371</b>
	Link and Multilink Services Overview	1371
<b>Chapter 58</b>	<b>Link and Multilink Services Configuration Guidelines</b>	<b>1375</b>
	Multilink and Link Services PICs Overview	1377
	Multilink Interfaces on Channelized MICs Overview	1379
	Understanding MLPPP Bundles and Link Fragmentation and Interleaving (LFI)	
	on Serial Links	1381
	Configuring the Number of Bundles on Link Services PICs	1383
	Configuring the Links in a Multilink or Link Services Bundle	1383
	Multilink and Link Services Logical Interface Configuration Overview	1385
	Default Settings for Multilink and Link Services Logical Interfaces	1385
	Configuring Encapsulation for Multilink and Link Services Logical Interfaces	1386
	Configuring the Drop Timeout Period on Multilink and Link Services Logical	
	Interfaces	1387

Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces . . . . .	1389
Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces . . . . .	1390
Configuring MRRU on Multilink and Link Services Logical Interfaces . . . . .	1391
Configuring the Sequence Header Format on Multilink and Link Services Logical Interfaces . . . . .	1392
Configuring DLCIs on Link Services Logical Interfaces . . . . .	1393
Configuring Point-to-Point DLCIs for MLFR FRF.16 and MLPPP Bundles . . . . .	1393
Configuring Multicast-Capable DLCIs for MLFR FRF.16 Bundles . . . . .	1393
Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces . . . . .	1394
Configuring LFI with DLCI Scheduling . . . . .	1395
Example: Configuring LFI with DLCI Scheduling . . . . .	1395
Configuring Link Services Physical Interfaces . . . . .	1397
Default Settings for Link Services Interfaces . . . . .	1397
Configuring Encapsulation for Link Services Physical Interfaces . . . . .	1398
Configuring Acknowledgment Timers on Link Services Physical Interfaces . . . . .	1399
Configuring Differential Delay Alarms on Link Services Physical Interfaces with MLFR FRF.16 . . . . .	1399
Configuring Keepalives on Link Services Physical Interfaces . . . . .	1400
Configuring CoS on Link Services Interfaces . . . . .	1401
CoS for Link Services Interfaces on M Series and T Series Routers . . . . .	1402
Example: Configuring CoS on Link Services Interfaces . . . . .	1403
Examples: Configuring Multilink Interfaces . . . . .	1406
Example: Configuring a Multilink Interface with MLPPP . . . . .	1407
Example: Configuring a Multilink Interface with MLPPP over ATM 2 Interfaces . . . . .	1408
Example: Configuring a Multilink Interface with MLFR FRF.15 . . . . .	1409
Examples: Configuring Link Interfaces . . . . .	1410
Example: Configuring a Link Services Interface with Two Links . . . . .	1411
Example: Configuring a Link Services Interface with MLPPP . . . . .	1412
Example: Configuring a Link Services Interface with MLFR FRF.15 . . . . .	1413
Example: Configuring a Link Services PIC with MLFR FRF.16 . . . . .	1413
Example: Configuring Link and Voice Services Interfaces with a Combination of Bundle Types . . . . .	1414
Example: Configuring an MLPPP Bundle . . . . .	1420
Example: Configuring Multilink Frame Relay FRF.15 . . . . .	1424
Example: Configuring Multilink Frame Relay FRF.16 . . . . .	1427
Example: Configuring Link Interfaces on Channelized MICs . . . . .	1430
<b>Chapter 59 Summary of Multilink and Link Services Configuration Statements . . . .</b>	<b>1441</b>
acknowledge-retries . . . . .	1442
acknowledge-timer . . . . .	1443
action-red-differential-delay . . . . .	1443
address (Interfaces) . . . . .	1444
bundle . . . . .	1444
destination (Interfaces) . . . . .	1445

	disable-mlppp-inner-ppp-pfc .....	1446
	dlci .....	1446
	drop-timeout .....	1447
	encapsulation .....	1448
	encapsulation (Logical Interface) .....	1448
	encapsulation (Physical Interface) .....	1449
	family .....	1450
	fragment-threshold .....	1451
	hello-timer .....	1451
	interfaces .....	1452
	interleave-fragments .....	1452
	lmi-type .....	1453
	minimum-links .....	1453
	mlfr-uni-nni-bundle-options .....	1454
	mrru .....	1455
	mtu .....	1456
	multicast-dlci .....	1456
	n391 .....	1457
	n392 .....	1458
	n393 .....	1459
	red-differential-delay .....	1459
	short-sequence .....	1460
	t391 .....	1460
	t392 .....	1461
	unit (Interfaces) .....	1462
	yellow-differential-delay .....	1463
<b>Part 7</b>	<b>Real-Time Performance Monitoring Services</b>	
<b>Chapter 60</b>	<b>Real-Time Performance Monitoring Services Overview .....</b>	<b>1467</b>
	Real-Time Performance Monitoring Services Overview .....	1467
	RFC 2544-Based Benchmarking Tests Overview .....	1468
<b>Chapter 61</b>	<b>Real-Time Performance Monitoring Configuration Guidelines .....</b>	<b>1471</b>
	[edit services rpm] Hierarchy Level .....	1471
	Configuring BGP Neighbor Discovery Through RPM .....	1473
	Configuring RPM Probes .....	1475
	Configuring RPM Receiver Servers .....	1480
	Limiting the Number of Concurrent RPM Probes .....	1481
	Configuring RPM Timestamping .....	1481
	Configuring TWAMP .....	1484
	Configuring TWAMP Interfaces .....	1485
	Configuring TWAMP Servers .....	1485
	Enabling RPM for the Junos OS extension-provider package .....	1486
	Tracing RPM Operations .....	1487
	Configuring the RPM Log File Name .....	1488
	Configuring the Number and Size of RPM Log Files .....	1488
	Configuring Access to the Log File .....	1488
	Configuring a Regular Expression for Lines to Be Logged .....	1488
	Configuring the Trace Operations .....	1489

## Chapter 62

Configuring an RFC 2544-Based Benchmarking Test .....	1489
Configuring a Test Name for an RFC 2544-Based Benchmarking Test for a IPv4 Network .....	1490
Configuring a Test Name for an RFC 2544-Based Benchmarking Test for an Ethernet Pseudowire: .....	1491
Example: Configuring an RFC 2544-Based Benchmarking Test for Layer 3 IPv4 Services .....	1492
Example: Configuring an RFC 2544-Based Benchmarking Test for UNI Direction of Ethernet Pseudowires .....	1500
Example: Configuring an RFC 2544-Based Benchmarking Test for NNI Direction of Ethernet Pseudowires .....	1507
Examples: Configuring BGP Neighbor Discovery Through RPM .....	1515
Examples: Configuring Real-Time Performance Monitoring .....	1516
<b>Summary of Real-Time Performance Monitoring Configuration Statements .....</b>	<b>1521</b>
authentication-mode .....	1521
bgp .....	1522
client-list .....	1523
data-fill .....	1523
data-size .....	1524
destination-ipv4-address (RFC 2544 Benchmarking) .....	1525
destination-interface .....	1526
destination-port .....	1527
destination-udp-port (RFC 2544 Benchmarking) .....	1528
direction (RFC 2544 Benchmarking) .....	1528
dscp-code-point .....	1529
family (RFC 2544 Benchmarking) .....	1530
hardware-timestamp .....	1531
history-size .....	1531
inactivity-timeout (Services RPM) .....	1532
logical-system .....	1532
max-connection-duration .....	1533
maximum-connections .....	1533
maximum-connections-per-client .....	1534
maximum-sessions .....	1534
maximum-sessions-per-connection .....	1535
mode (RFC 2544 Benchmarking) .....	1535
moving-average-size .....	1536
one-way-hardware-timestamp .....	1536
port .....	1537
port (RPM) .....	1537
port (TWAMP) .....	1537
probe .....	1538
probe-count .....	1539
probe-interval .....	1539
probe-limit .....	1540
probe-server .....	1541
probe-type .....	1542

	routing-instance . . . . .	1543
	routing-instances . . . . .	1543
	rfc2544-benchmarking . . . . .	1544
	rpm . . . . .	1545
	server . . . . .	1546
	server-inactivity-timeout . . . . .	1546
	services (RPM) . . . . .	1547
	source-address . . . . .	1547
	source-ipv4-address (RFC 2544 Benchmarking) . . . . .	1548
	source-udp-port (RFC 2544 Benchmarking) . . . . .	1548
	target (Services RPM) . . . . .	1549
	tcp . . . . .	1549
	test . . . . .	1550
	tests (RFC 2544 Benchmarking) . . . . .	1551
	test-interface (RFC 2544 Benchmarking) . . . . .	1552
	test-name (RFC 2544 Benchmarking) . . . . .	1553
	test-interval . . . . .	1554
	traceoptions (RPM) . . . . .	1555
	thresholds . . . . .	1556
	traps . . . . .	1557
	twamp . . . . .	1558
	twamp-server . . . . .	1559
	udp . . . . .	1559
<b>Part 8</b>	<b>Tunnel Services</b>	
<b>Chapter 63</b>	<b>Tunnel Services Overview . . . . .</b>	<b>1563</b>
	Tunnel Services Overview . . . . .	1563
	GRE Keepalive Time Overview . . . . .	1566
<b>Chapter 64</b>	<b>Tunnel Interfaces Configuration Guidelines . . . . .</b>	<b>1567</b>
	Configuring Unicast Tunnels . . . . .	1567
	Configuring a Key Number on GRE Tunnels . . . . .	1570
	Enabling Fragmentation on GRE Tunnels . . . . .	1570
	Specifying an MTU Setting for the Tunnel . . . . .	1571
	Configuring a GRE Tunnel to Copy ToS Bits to the Outer IP Header . . . . .	1571
	Configuring Packet Reassembly . . . . .	1572
	Configuring GRE Keepalive Time . . . . .	1573
	Configuring Keepalive Time and Hold time for a GRE Tunnel Interface . . . . .	1573
	Display GRE Keepalive Time Configuration . . . . .	1574
	Display Keepalive Time Information on a GRE Tunnel Interface . . . . .	1574
	Restricting Tunnels to Multicast Traffic . . . . .	1575
	Configuring Logical Tunnel Interfaces . . . . .	1576
	Connecting Logical Systems . . . . .	1576
	Configuring Tunnel Interfaces for Routing Table Lookup . . . . .	1577
	Configuring Virtual Loopback Tunnels for VRF Table Lookup . . . . .	1578
	Configuring PIM Tunnels . . . . .	1580
	Configuring IPv6-over-IPv4 Tunnels . . . . .	1580
	Configuring IPv4-over-IPv6 Tunnels . . . . .	1581
	Configuring Dynamic Tunnels . . . . .	1581

	Configuring Tunnel Interfaces on MX Series Routers . . . . .	1582
	Configuring Tunnel Interfaces on T4000 Routers . . . . .	1583
	Examples: Configuring Unicast Tunnels . . . . .	1584
	Example: Configuring a Virtual Loopback Tunnel for VRF Table Lookup . . . . .	1586
	Example: Configuring an IPv6-over-IPv4 Tunnel . . . . .	1586
	Example: Configuring an IPv4-over-IPv6 Tunnel . . . . .	1587
	Example: Configuring Logical Tunnels . . . . .	1589
<b>Chapter 65</b>	<b>Summary of Tunnel Services Configuration Statements . . . . .</b>	<b>1591</b>
	allow-fragmentation . . . . .	1591
	backup-destination . . . . .	1592
	copy-tos-to-outer-ip-header . . . . .	1592
	destination . . . . .	1593
	destination (Tunnel Remote End) . . . . .	1593
	destination (Routing Instance) . . . . .	1593
	destination-networks . . . . .	1594
	do-not-fragment . . . . .	1595
	dynamic-tunnels . . . . .	1596
	hold-time (OAM) . . . . .	1597
	interfaces . . . . .	1597
	keepalive-time . . . . .	1598
	key . . . . .	1599
	multicast-only . . . . .	1599
	peer-unit . . . . .	1600
	reassemble-packets . . . . .	1600
	routing-instance . . . . .	1601
	routing-instances . . . . .	1601
	routing-options . . . . .	1602
	source . . . . .	1602
	source-address . . . . .	1603
	ttl . . . . .	1603
	tunnel . . . . .	1604
	unit (Interfaces) . . . . .	1605
<b>Part 9</b>	<b>Index</b>	
	Index . . . . .	1609
	Index of Statements and Commands . . . . .	1635

# List of Figures

<b>Part 2</b>	<b>Adaptive Services</b>	
<b>Chapter 3</b>	<b>Adaptive Services Overview . . . . .</b>	<b>39</b>
	Figure 1: Packet Flow Through the Adaptive Services or MultiServices PIC . . . . .	48
	Figure 2: IPv4 Depletion Solution - IPv4 Access Network . . . . .	52
	Figure 3: IPv4 Depletion Solution - IPv6 Access Network . . . . .	53
	Figure 4: Dynamic NAT Flow . . . . .	57
	Figure 5: Stateful NAT64 Flow . . . . .	58
	Figure 6: DS-Lite Flow . . . . .	58
	Figure 7: Supported Inline NAT Types . . . . .	59
	Figure 8: Basic PCP NAPT44 Topology . . . . .	65
	Figure 9: PCP with DS-Lite Plain Mode . . . . .	66
	Figure 10: PCP with DS-Lite Tunnel Mode . . . . .	66
	Figure 11: 6rd Software Flow . . . . .	75
<b>Chapter 6</b>	<b>Network Address Translation Configuration Guidelines . . . . .</b>	<b>191</b>
	Figure 12: Configuring NAT for Multicast Traffic . . . . .	247
	Figure 13: Configuring DNS ALGs with NAT-PT Network Topology . . . . .	269
	Figure 14: Deploy Inline NAT within L3VPN . . . . .	283
	Figure 15: PCP with NAPT44 . . . . .	290
<b>Chapter 8</b>	<b>Software Configuration Guidelines . . . . .</b>	<b>343</b>
	Figure 16: DS-Lite Topology . . . . .	348
<b>Chapter 19</b>	<b>IPsec Services Configuration Guidelines . . . . .</b>	<b>479</b>
	Figure 17: IPsec Dynamic Endpoint Tunneling Topology . . . . .	524
<b>Part 4</b>	<b>Encryption Services</b>	
<b>Chapter 47</b>	<b>Encryption Interfaces Configuration Guidelines . . . . .</b>	<b>1101</b>
	Figure 18: Example: IPsec Tunnel Connecting Security Gateways . . . . .	1103
	Figure 19: IPsec Tunnel Redundancy . . . . .	1110
<b>Part 5</b>	<b>Flow Monitoring and Discard Accounting Services</b>	
<b>Chapter 49</b>	<b>Flow Monitoring and Discard Accounting Overview . . . . .</b>	<b>1123</b>
	Figure 20: Passive Monitoring Application Topology . . . . .	1124
	Figure 21: Active Monitoring Configuration Topology . . . . .	1127
<b>Chapter 50</b>	<b>Flow Monitoring and Discard Accounting Configuration Guidelines . . . .</b>	<b>1129</b>
	Figure 22: Configuring Sampling Rate . . . . .	1136
<b>Chapter 52</b>	<b>Flow Collection Configuration Guidelines . . . . .</b>	<b>1295</b>

	Figure 23: Flow Collector Interface Topology Diagram . . . . .	1301
<b>Chapter 54</b>	<b>Dynamic Flow Capture Configuration Guidelines . . . . .</b>	<b>1327</b>
	Figure 24: Junos Capture Vision Topology . . . . .	1328
<b>Chapter 55</b>	<b>Flow-Tap Configuration Guidelines . . . . .</b>	<b>1339</b>
	Figure 25: Junos Packet Vision Topology . . . . .	1341
<b>Part 6</b>	<b>Link and Multilink Services</b>	
<b>Chapter 58</b>	<b>Link and Multilink Services Configuration Guidelines . . . . .</b>	<b>1375</b>
	Figure 26: Multilink Interface Configuration . . . . .	1384
	Figure 27: Configuring MLPPP and LFI on Serial Links . . . . .	1421
<b>Part 7</b>	<b>Real-Time Performance Monitoring Services</b>	
<b>Chapter 61</b>	<b>Real-Time Performance Monitoring Configuration Guidelines . . . . .</b>	<b>1471</b>
	Figure 28: RFC 2544-Based Benchmarking Test for a Layer 3 IPv4 Service . . . .	1493
	Figure 29: RFC 2544-Based Benchmarking Test for UNI Direction of an Ethernet Pseudowire . . . . .	1501
	Figure 30: RFC 2544-Based Benchmarking Test for NNI Direction of an Ethernet Pseudowire . . . . .	1508
<b>Part 8</b>	<b>Tunnel Services</b>	
<b>Chapter 64</b>	<b>Tunnel Interfaces Configuration Guidelines . . . . .</b>	<b>1567</b>
	Figure 31: IPv6 Tunnel Connecting Two IPv4 Networks Across an IPv6 Network . . . . .	1587

# List of Tables

	<b>About This Guide</b> . . . . .	<b>xliv</b>
	Table 1: Notice Icons . . . . .	liii
	Table 2: Text and Syntax Conventions . . . . .	liii
<b>Part 2</b>	<b>Adaptive Services</b>	
<b>Chapter 3</b>	<b>Adaptive Services Overview</b> . . . . .	<b>39</b>
	Table 3: AS and Multiservices PIC Services by Service Package, PIC, and Platform . . . . .	43
	Table 4: Carrier-Grade NAT—Feature Comparison by Platform . . . . .	60
	Table 5: Carrier-Grade NAT Translation Types . . . . .	61
	Table 6: ALGs Available by Default . . . . .	63
	Table 7: Carrier-Grade NAT—Feature Comparison by Platform . . . . .	67
	Table 8: Carrier-Grade NAT Translation Types . . . . .	68
	Table 9: ALGs Available by Default . . . . .	69
	Table 10: Statement Equivalents for ES and AS Interfaces . . . . .	77
	Table 11: MX Series Routers that Support MS-MIC and MS-MPC . . . . .	83
	Table 12: Quick Reference to Key Configuration Statements at This Hierarchy Level . . . . .	89
	Table 13: Quick Reference to Configuration Statements at This Hierarchy Level . . . . .	89
	Table 14: Quick Reference to Key Configuration Statements at this Hierarchy Level . . . . .	90
	Table 15: Key Configuration Statements Used in this Example . . . . .	97
<b>Chapter 4</b>	<b>Applications Configuration Guidelines</b> . . . . .	<b>125</b>
	Table 16: ALGs Supported by the Junos OS . . . . .	126
	Table 17: RealAudio Product Port Usage . . . . .	132
	Table 18: Supported RPC Services . . . . .	133
	Table 19: Application Protocols Supported by Services Interfaces . . . . .	147
	Table 20: Network Protocols Supported by Services Interfaces . . . . .	149
	Table 21: ICMP Codes and Types Supported by Services Interfaces . . . . .	151
	Table 22: Port Names Supported by Services Interfaces . . . . .	152
	Table 23: Requesting Messages with NAT Table . . . . .	160
<b>Chapter 6</b>	<b>Network Address Translation Configuration Guidelines</b> . . . . .	<b>191</b>
	Table 24: Deterministic Port Block Allocation Commit Constraints . . . . .	203
	Table 25: Comparison of NAPT Implementation Methods . . . . .	203
<b>Chapter 11</b>	<b>Stateful Firewall Services Configuration Guidelines</b> . . . . .	<b>387</b>
	Table 26: IP Option Values . . . . .	391

<b>Chapter 16</b>	<b>Summary of Load Balancing Configuration Statements . . . . .</b>	<b>431</b>
	Table 27: Behavior of Member Interface After One Multiservices PIC Fails . . . . .	438
	Table 28: Behavior of Member Interface After Two Multiservices PICs Fail . . . . .	439
<b>Chapter 19</b>	<b>IPsec Services Configuration Guidelines . . . . .</b>	<b>479</b>
	Table 29: Default IKE and IPsec Proposals for Dynamic Negotiations . . . . .	517
<b>Chapter 21</b>	<b>Layer 2 Tunneling Protocol Services Configuration Guidelines . . . . .</b>	<b>577</b>
	Table 30: System Log Message Severity Levels . . . . .	585
<b>Chapter 29</b>	<b>Service Set Configuration Guidelines . . . . .</b>	<b>741</b>
	Table 31: System Log Message Severity Levels . . . . .	755
	Table 32: Adaptive Services Tracing Flags . . . . .	758
<b>Chapter 31</b>	<b>Service Interface Configuration Guidelines . . . . .</b>	<b>795</b>
	Table 33: System Log Message Severity Levels . . . . .	801
<b>Part 5</b>	<b>Flow Monitoring and Discard Accounting Services</b>	
<b>Chapter 50</b>	<b>Flow Monitoring and Discard Accounting Configuration Guidelines . . . . .</b>	<b>1129</b>
	Table 34: Values of Template and Option Template IDs for IPFIX Flows . . . . .	1168
	Table 35: Values of Template and Option Template IDs for Version 9 Flows . . . . .	1169
	Table 36: Values of Template and Option Template IDs for IPFIX Flows . . . . .	1170
	Table 37: Example of Observation Domain ID . . . . .	1173
<b>Part 6</b>	<b>Link and Multilink Services</b>	
<b>Chapter 58</b>	<b>Link and Multilink Services Configuration Guidelines . . . . .</b>	<b>1375</b>
	Table 38: Multilink and Link Services PIC Capacities . . . . .	1377
	Table 39: Multilink and Link Services Logical Interface Statements . . . . .	1385
	Table 40: Link Services Physical Interface Statements for MLFR FRF.16 . . . . .	1398
	Table 41: Link Services CoS Queues . . . . .	1402
	Table 42: Link Services Bundle . . . . .	1411
<b>Part 7</b>	<b>Real-Time Performance Monitoring Services</b>	
<b>Chapter 60</b>	<b>Real-Time Performance Monitoring Services Overview . . . . .</b>	<b>1467</b>
	Table 43: Supported Network Topologies for RFC 2544 Benchmarking Tests . . . . .	1469
<b>Chapter 61</b>	<b>Real-Time Performance Monitoring Configuration Guidelines . . . . .</b>	<b>1471</b>
	Table 44: RPM Tracing Flags . . . . .	1489
<b>Part 8</b>	<b>Tunnel Services</b>	
<b>Chapter 63</b>	<b>Tunnel Services Overview . . . . .</b>	<b>1563</b>
	Table 45: Tunnel Interface Types . . . . .	1563
<b>Chapter 64</b>	<b>Tunnel Interfaces Configuration Guidelines . . . . .</b>	<b>1567</b>
	Table 46: Methods for Configuring Egress Filtering . . . . .	1578

# About This Guide

This preface provides the following guidelines for using the *Junos<sup>®</sup> OS Services Interfaces Configuration Guide*:

- [Junos Documentation and Release Notes on page xlix](#)
- [Objectives on page l](#)
- [Audience on page l](#)
- [Supported Platforms on page l](#)
- [Using the Indexes on page li](#)
- [Using the Examples in This Manual on page li](#)
- [Documentation Conventions on page lii](#)
- [Documentation Feedback on page liv](#)
- [Requesting Technical Support on page lv](#)

## Junos Documentation and Release Notes

---

For a list of related Junos documentation, see <http://www.juniper.net/techpubs/software/junos/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Release Notes*.

To obtain the most current version of all Juniper Networks<sup>®</sup> technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

## Objectives

---

This guide provides an overview of the services interfaces provided by Junos OS and describes how to configure these properties on the router.



**NOTE:** For additional information about the Junos OS—either corrections to or information that might have been omitted from this guide—see the software release notes at <http://www.juniper.net/>.

---

## Audience

---

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks M Series, MX Series, T Series, EX Series, or J Series router or switch.

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

## Supported Platforms

---

For the features described in this manual, the Junos OS currently supports the following platforms:

- J Series
- M Series

- MX Series
- SRX Series
- T Series
- EX Series

## Using the Indexes

---

This reference contains two indexes: a complete index that includes topic entries, and an index of statements and commands only.

In the index of statements and commands, an entry refers to a statement summary section only. In the complete index, the entry for a configuration statement or command contains at least two parts:

- The primary entry refers to the statement summary section.
- The secondary entry, *usage guidelines*, refers to the section in a configuration guidelines chapter that describes how to use the statement or command.

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

## Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
```

```
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

---

## Documentation Conventions

Table 1 on page liii defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page liii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"><li>To configure a stub area, include the <b>stub</b> statement at the <b>[edit protocols ospf area area-id]</b> hierarchy level.</li><li>The console port is labeled <b>CONSOLE</b>.</li></ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric <i>metric</i>&gt;;</b>
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <b>(<i>string1</i>   <i>string2</i>   <i>string3</i>)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options {   static {     route default {       nexthop <i>address</i>;       retain;     }   } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
<b>GUI Conventions</b>		
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"><li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li><li>To cancel the configuration, click <b>Cancel</b>.</li></ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>.

- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at <http://www.juniper.net/support/requesting-support.html>

## PART 1

# Overview

- [Services Interfaces Overview on page 3](#)
- [Services Interfaces Configuration Statements on page 7](#)



## CHAPTER 1

# Services Interfaces Overview

This chapter includes the following topics:

- [Understanding Services PICs on page 3](#)
- [Supported Platforms on page 5](#)

## Understanding Services PICs

---

Interfaces used in router networks can be broadly classified into two:

- Networking interfaces, such as Ethernet and SONET interfaces, that primarily provide traffic connectivity. For more information on these interfaces, see the Junos<sup>®</sup> OS Network Interfaces.
- Services interfaces, such as Adaptive Services interfaces and Multiservices interfaces, that provide specific capabilities for manipulating traffic before it is delivered to its destination.

Services interfaces enable you to add services to your network incrementally. TJunos OS supports the following services interfaces:

- [Adaptive services and Multiservices PICs on page 3](#)
- [Encryption Services \(ES\) PIC on page 4](#)
- [Multilink Services and Link Services PICs on page 4](#)
- [Monitoring Services PICs on page 4](#)
- [Tunnel Services PIC on page 5](#)
- [Multiservices MIC and Multiservices MPC on page 5](#)

## Adaptive services and Multiservices PICs

Adaptive Services [AS] PICs and Multiservices PICs enable you to perform multiple services on the same PIC by configuring a set of services and applications. The AS and Multiservices PICs offer a range of services that you can configure in one or more service sets. The following are some of the services you can configure on Adaptive services or multiservices interfaces:

- Class-of-service
- Intrusion detection service (IDS)

- IP Security (IPsec)
- Layer 2 tunneling protocols
- Monitoring services
- Network Address Translation (NAT)
- Stateful firewalls
- Voice services

For more information about these services, see [“Adaptive Services Overview” on page 39](#).



**NOTE:** On Juniper Networks MX Series 3D Universal Edge Routers, the Multiservices DPC provides essentially the same capabilities as the Multiservices PIC. The interfaces on both platforms are configured in the same way.

## Encryption Services (ES) PIC

ES PIC provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. It also defines mechanisms for key generation and exchange, management of security associations, and support for digital certificates. For more information about encryption interfaces, see [“Configuring Encryption Interfaces” on page 1101](#).

## Multilink Services and Link Services PICs

Multilink Services and Link Services PICs enable you to split, recombine, and sequence datagrams across multiple logical data links. The goal of multilink operation is to coordinate multiple independent links between a fixed pair of systems, providing a virtual link with greater bandwidth than any of the members. The Junos OS supports two services PICs based on the Multilink Protocol: the Multilink Services PIC and the Link Services PIC.

For more information about multilink and link services interfaces, see *Link and Multilink Properties*.

## Monitoring Services PICs

Monitoring Services PICs enable you to monitor traffic flow and export the monitored traffic. Monitoring traffic allows you to perform the following tasks:

- Gather and export detailed information about IPv4 traffic flows between source and destination nodes in your network.
- Sample all incoming IPv4 traffic on the monitoring interface and present the data in cflowd record format.
- Perform discard accounting on an incoming traffic flow.

- Encrypt or tunnel outgoing cflowd records, intercepted IPv4 traffic, or both.
- Direct filtered traffic to different packet analyzers and present the data in its original format.

For more information about flow monitoring interfaces, see *Flow Monitoring*.

## Tunnel Services PIC

Tunnel Services PIC provides a private, secure path through an otherwise public network by encapsulating arbitrary packets inside a transport protocol. Tunnels connect discontinuous subnetworks and enable encryption interfaces, virtual private networks (VPNs), and MPLS.

For more information about tunnel interfaces, see *Tunnel Properties*.

## Multiservices MIC and Multiservices MPC

The Multiservices Modular Interfaces Card (MS-MIC) and the Multiservices Modular PIC Concentrator (MS-MPC), introduced in Junos OS Release 13.2, provide improved scaling and high performance. The MS-MIC and MS-MPC have enhanced memory (16 GB for MS-MIC, 32 GB per NPU of MS-MPC) and processing capabilities.

The services interfaces on MS-MPC and MS-MIC are identified in the configuration with an **ms-** prefix (for example, **ms-1/2/1**).

The following services packages come preinstalled and preconfigured on MS-MICs and MS-MPCs in Junos OS Release 13.2:

- Junos Traffic Vision (formerly referred to as Jflow/Flow Monitoring)
- Junos Address Aware (formerly referred to as NAT features)
- Junos VPN Site Secure (formerly referred to as IPsec features)
- Junos Network Secure (formerly referred to as the Stateful Firewall feature)

For information about MS-MIC and MS-MPC, see *Introducing Multiservices MIC and Multiservices MPC (MS-MIC and MS-MPC)*.

### Related Documentation

- [Supported Platforms on page 5](#)
- [Packet Flow Through the Adaptive Services or Multiservices PIC on page 47](#)
- [Enabling Service Packages on page 41](#)
- [Services Configuration Procedure on page 46](#)
- [Services Interface Naming Overview on page 797](#)

## Supported Platforms

For information about which platforms support Adaptive Services and MultiServices PICs and their features, see [“Enabling Service Packages” on page 41](#).

For information about PIC support on a specific Juniper Networks M Series Multiservice Edge Router or T Series Core Router, see the appropriate *PIC Guide* for the platform.

For information about MS-DPC support on a specific MX Series router, see the appropriate *DPC Guide* for the platform.

For information about services supported on Juniper Networks SRX Series Services Gateways and J Series Services Routers, see the *Junos OS Feature Support Reference for SRX Series and J Series Devices*.

**Related  
Documentation**

- [Understanding Services PICs on page 3](#)
- *Introducing Multiservices MIC and Multiservices MPC (MS-MIC and MS-MPC)*

## CHAPTER 2

# Services Interfaces Configuration Statements

This chapter shows the complete configuration statement hierarchies for configuring services interfaces. It lists all the statements that pertain to configuring services and shows the `user@host#` level in the configuration hierarchy. When you are configuring the Junos OS, your current hierarchy level is shown in the banner on the line preceding the `user@host#` prompt.

For a complete list of the Junos configuration statements, see the *Junos OS Hierarchy and RFC Reference*.

This chapter is organized as follows:

- [\[edit applications\] Hierarchy Level on page 7](#)
- [\[edit forwarding-options\] Hierarchy Level on page 8](#)
- [\[edit interfaces\] Hierarchy Level on page 10](#)
- [\[edit logical-systems\] Hierarchy Level on page 14](#)
- [\[edit services\] Hierarchy Level on page 14](#)

### [\[edit applications\] Hierarchy Level](#)

---

To configure application protocols, include the following statements at the **[edit applications]** hierarchy level of the configuration:

```
application application-name {  
  application-protocol protocol-name;  
  destination-port port-number;  
  icmp-code value;  
  icmp-type value;  
  inactivity-timeout value;  
  learn-sip-register;  
  protocol type;  
  rpc-program-number number;  
  sip-call-hold-timeout seconds;  
  snmp-command command;  
  source-port port-number;  
  ttl-threshold value;  
  uuid hex-value;
```

```

}
application-set application-set-name {
  application application-name;
}

```

## [edit forwarding-options] Hierarchy Level

To configure flow monitoring and accounting properties, include the following statements at the [edit forwarding-options] hierarchy level:



**NOTE:** For the complete [edit forwarding-options] hierarchy, see the *Routing Policy Feature Guide for Routing Devices*. This listing includes only the statements used in flow monitoring and accounting services.

```

accounting name {
  output {
    aggregate-export-interval seconds;
    cflowd hostname {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
      autonomous-system-type (origin | peer);
      port port-number;
      version format;
    }
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    interface interface-name {
      engine-id number;
      engine-type number;
      source-address address;
    }
  }
}
monitoring name {
  family inet {
    output {
      cflowd hostname port port-number;
      export-format format;
      flow-active-timeout seconds;
      flow-export-destination {
        collector-pic;
      }
      flow-inactive-timeout seconds;
      interface interface-name {
        engine-id number;
        engine-type number;
      }
    }
  }
}

```

```

        input-interface-index number;
        output-interface-index number;
        source-address address;
    }
}
}
next-hop-group group-name {
    interface interface-name {
        next-hop address;
    }
}
port-mirroring {
    input {
        rate rate;
        run-length number;
    }
    family (inet | inet6) {
        input {
            rate rate;
            run-length number;
        }
        output {
            interface interface-name {
                next-hop address;
            }
            no-filter-check;
        }
    }
}
traceoptions {
    file filename {
        files number;
        size bytes;
        (world-readable | no-world-readable);
    }
}
}
sampling {
    disable;
    family (inet | inet6 | mpls) {
        max-packets-per-second number;
        rate number;
        run-length number;
    }
    input {
        rate number;
        run-length number;
    }
    output {
        aggregate-export-interval seconds;
        cflowd hostname {
            aggregation {
                autonomous-system;
                destination-prefix;
                protocol-port;
                source-destination-prefix {
                    caida-compliant;
                }
            }
        }
    }
}

```

```

    }
    source-prefix;
  }
  autonomous-system-type (origin | peer);
  version9 {
    template template-name;
  }
  (local-dump | no-local-dump);
  port port-number;
  source-address address;
  version format;
}
file {
  disable;
  filename filename;
  files number;
  size bytes;
  (stamp | no-stamp);
  (world-readable | no-world-readable);
}
flow-active-timeout seconds;
flow-inactive-timeout seconds;
interface interface-name {
  engine-id number;
  engine-type number;
  source-address address;
}
}
traceoptions (Forwarding Options) {
  file filename {
    files number;
    size bytes;
    (world-readable | no-world-readable);
  }
}
}
}

```

## [edit interfaces] Hierarchy Level

To configure services interfaces, include the following statements at the **[edit interfaces]** hierarchy level of the configuration. The statements can also be configured at the **[edit logical-systems logical-system-name interfaces]** hierarchy level.



**NOTE:** For the complete **[edit interfaces]** hierarchy, see the *Junos OS Network Interfaces Library for Routing Devices*. This listing includes only the statements used in configuring services.

```

[edit interfaces]
interface-name {
  (atm-options | fastether-options | gige-ether-options | sonet-options) {
    mpls {
      pop-all-labels {
        required-depth number;
      }
    }
  }
}

```

```

    }
  }
}
encapsulation type;
lsq-failure-options {
  no-termination-request;
  trigger-link-failure interface-name;
}
mlfr-uni-nni-bundle-options {
  acknowledge-retries number;
  acknowledge-timer milliseconds;
  action-red-differential-delay (disable-tx | remove-link);
  drop-timeout milliseconds;
  fragment-threshold bytes;
  cisco-interoperability send-lip-remove-link-for-link-reject;
  hello-timer milliseconds;
  lmi-type (ansi | itu);
  minimum-links number;
  mrru bytes;
  n391 number;
  n392 number;
  n393 number;
  red-differential-delay milliseconds;
  t391 number;
  t392 number;
  yellow-differential-delay milliseconds;
  encapsulation type;
}
passive-monitor-mode;
unit logical-unit-number {
  clear-dont-fragment-bit;
  compression {
    rtp {
      f-max-period number;
      maximum-contexts number <force>;
      port {
        minimum port-number;
        maximum port-number;
      }
      queues [ queue-numbers ];
    }
  }
}
compression-device interface-name;
copy-tos-to-outer-ip-header;
disable-mlppp-inner-ppp-pfc;
dlci dlci-identifier;
drop-timeout milliseconds;
dial-options {
  ipsec-interface-id name;
  l2tp-interface-id name;
  (dedicated | shared);
}
encapsulation type;
family family {
  accounting {
    destination-class-usage;

```

```

        source-class-usage direction;
    }
    address address {
        destination address;
    }
    bundle (ml-fpc/pic/port | ls-fpc/pic/port);
    ipsec-sa ipsec-sa;
    multicast-only;
    receive-options-packets;
    receive-ttl-exceeded;
    sampling direction;
    service {
        input {
            service-set service-set-name <service-filter filter-name>;
            post-service-filter filter-name;
        }
        output {
            service-set service-set-names <service-filter filter-name>;
        }
    }
}
fragment-threshold bytes;
interleave-fragments;
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
peer-unit unit-number;
reassemble-packets;
rpm ;
service-domain (inside | outside);
short-sequence;
tunnel {
    allow-fragmentation;
    backup-destination address;
    destination destination-address;
    do-not-fragment;
    key number;
    routing-instance {
        destination routing-instance-name;
    }
    source-address address;
    ttl number;
}
twamp-server;
}
multiservice-options {
    (core-dump | no-core-dump);
    (syslog | no-syslog);
    flow-control-options {
        down-on-flow-control;
        dump-on-flow-control;
        reset-on-flow-control;
    }
}
}
services-options {
    cgn-pic;

```

```

close-timeout
disable-global-timeout-override;
ignore-errors <alg> <tcp>;
inactivity-non-tcp-timeout seconds;
inactivity-tcp-timeout seconds;
inactivity-timeout seconds;
open-timeout seconds;
session-limit {
    maximum number;
    rate new-sessions-per-second;
}
session-timeout seconds;
syslog {
    host hostname {
        facility-override facility-name;
        log-prefix prefix-value;
        port port-number;
        services severity-level;
    }
    message-rate-limit messages-per-second;
}
tcp-tickles tcp-tickles;
}
}
rlsnumber {
    redundancy-options {
        hot-standby | warm-standby;
        primary lsq-fpc/pic/port;
        secondary lsq-fpc/pic/port;
    }
}
rlsnumber:number {
    redundancy-options {
        hot-standby | warm-standby;
        primary lsq-fpc/pic/port;
        secondary lsq-fpc/pic/port;
    }
}
encapsulation multilink-frame-relay-uni-nni;
unit logical-unit-number {
    encapsulation multilink-frame-relay-end-to-end;
}
}
}
rspnumber {
    redundancy-options {
        primary sp-fpc/pic/port;
        secondary sp-fpc/pic/port;
        hot-standby;
    }
}
}
so-fpc/pic/port {
    unit logical-unit-number {
        passive-monitor-mode;
    }
}
}

```

## [edit logical-systems] Hierarchy Level

---

The following lists the statements that can be configured at the **[edit logical-systems]** hierarchy level that are documented in this manual. For more information about logical systems, see the *Junos OS Routing Protocols Library for Routing Devices*.

```
logical-system-name {  
  interfaces interface-name {  
    interface-configuration;  
  }  
}
```

## [edit services] Hierarchy Level

---

To configure services, include the following statements at the **[edit services]** hierarchy level of the configuration:



**NOTE:** For the complete **[edit services]** hierarchy, see the *Junos OS Hierarchy and RFC Reference*. This listing includes only the statements documented in this manual; additional statements are documented in the *Junos OS Subscriber Management and Services Library*.

```
acl {  
  rule rule-name {  
    match-direction (input | output | input-output);  
    term term-name {  
      from {  
        application-group-any;  
        application-groups [ application-group-names ];  
        application-unknown;  
        applications [ application-names ];  
        destination-address address <any-unicast>;  
        destination-address-range low minimum-value high maximum-value;  
        destination-prefix-list list-name;  
        source-address address <any-unicast>;  
        source-address-range low minimum-value high maximum-value;  
        source-prefix-list list-name;  
      }  
      then {  
        (accept | discard);  
        count (application | application-group | application-group-any | none);  
        forwarding-class class-name;  
        policer policer-name;  
      }  
    }  
  }  
  rule-set rule-set-name {  
    [ rule rule-names ];  
  }  
}  
adaptive-services-pics {
```

```

traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
        regex>;
    flag flag;
    no-remote-trace;
}
}
application-identification {
    application application-name {
        disable;
        enable-heuristics;
        idle-timeout seconds;
        index number;
        session-timeout seconds;
        type type;
        type-of-service service-type;
        port-mapping {
            port-range {
                tcp (port | range);
                udp (port | range);
            }
            disable;
        }
    }
}
application-group group-name {
    disable;
    application-groups {
        name [application-group-name];
    }
    applications {
        name [application-name];
    }
    index number;
}
application-system-cache-timeout seconds;
max-checked-bytes bytes;
min-checked-bytes bytes;
nested-application
nested-application-settings
no-application-identification;
no-application-system-cache;
no-clear-application-system-cache;
no-signature-based;
profile profile-name {
    [ rule-set rule-set-name ];
}
rule rule-name {
    disable;
    address address-name {
        destination {
            ip address</prefix-length>;
            port-range {
                tcp [ ports-and-port-ranges ];
                udp [ ports-and-port-ranges ];
            }
        }
    }
}

```

```

    source {
        ip address </prefix-length>;
        port-range {
            tcp [ ports-and-port-ranges ];
            udp [ ports-and-port-ranges ];
        }
    }
    order number;
}
application application-name;
}
rule-set rule-set-name {
    rule application-rule-name;
}
}
traceoptions {
    file filename <files number> <match regex> <size size> <world-readable |
        no-world-readable>;
    flag flag;
    no-remote-trace;
}
}
border-signaling-gateway {
    gateway gateway-name {
        admission-control admission-control-profile {
            dialogs {
                maximum-concurrent number;
                committed-attempts-rate dialogs-per-second;
                committed-burst-size number-of-dialogs;
            }
            transactions {
                maximum-concurrent number;
                committed-attempts-rate transactions-per-second;
                committed-burst-size number-of-transactions;
            }
        }
    }
}
embedded-spdp {
    service-class service-class-name {
        term term-name {
            from {
                media-type (any-media | audio | video);
            }
            then {
                committed-burst-size bytes;
                committed-information-rate bytes-per-second;
                dscp (alias | do-not-change | dscp-value);
                reject;
            }
        }
    }
}
}
service-point service-point-name {
    default-media-realm
    service-interface interface-name.unit-number;
    service-point-type service-point-type;
    service-policies {
        new-call-usage-input-policies [policy-and-policy-set-names];
    }
}

```

```

new-call-usage-output-policies [policy-and-policy-set-names];
new-transaction-input-policies [policy-and-policy-set-names];
new-transaction-output-policies [policy-and-policy-set-names];
}
transport-details <port port-number> <ip-address ip-address> <tcp> <udp>;
}
sip {
  message-manipulation-rules {
    manipulation-rule rule-name {
      actions {
        sip-header header-field-name {
          field-value {
            modify-regular-expression regular-expression with field-value;
            add field-value;
            add-missing field-value;
            add-overwrite field-value;
            remove-regular-expression regular-expression;
            remove-all;
            reject-regular-expression regular-expression;
          }
        }
      }
      request-uri request-uri {
        field-value {
          modify-regular-expression regular-expression with field-value;
        }
      }
    }
  }
}
new-call-usage-policy policy-name {
  term term-name {
    from {
      contact [ contact-fields ];
      method {
        method-invite;
      }
      request-uri [ uri-fields ];
      source-address [ ip-addresses ];
    }
    then {
      media-policy {
        data-inactivity-detection (Services PGCP) {
          inactivity-duration (Services Border Signaling Gateway) seconds;
        }
        no-anchoring;
        service-class service-class-name;
      }
      trace;
    }
  }
}
new-call-usage-policy-set policy-set-name {
  policy-name [ policy-names ];
}
new-transaction-policy policy-name {
  term term-name {
    from {

```

```

    contact {
        registration-state [ registered | not-registered ];
        regular-expression [ regular-expression ];
        uri-hiding [ hidden-uri | not-hidden-uri ];
    }
    method {
        method-invite;
        method-message;
        method-options;
        method-publish;
        method-refer;
        method-register;
        method-subscribe;
    }
    request-uri {
        registration-state [ registered | not-registered ];
        regular-expression [ regular-expression ];
        uri-hiding [ hidden-uri | not-hidden-uri ];
    }
    source-address [ ip-addresses ];
}
then {
    (accept | reject);
    admission-control admission-control-profile;
    message-manipulation {
        forward-manipulation {
            manipulation-rule-name;
        }
        reverse-manipulation {
            manipulation-rule-name;
        }
    }
}
on-3xx-response{
    recursion-limit number;
}
}
route (Services) {
    egress-service-point service-point-name;
    next-hop (Services) (request-uri | address ipv4-address | <port port-number>
        <transport-protocol (udp | tcp)>);
    server-cluster cluster-name;
}
signaling-realm signaling-realm;
trace;
}
}
}
new-transaction-policy-set policy-set-name {
    policy-name [ policy-names ];
}
routing-destinations {
    availability-check-profiles {
        profile-name;
    }
    keepalive-interval {
        available-server seconds;
        unavailable-server seconds;
    }
}

```

```

    }
    keepalive-method sip-options;
    keepalive-strategy (do-not-send <blackout-period seconds> | send-always <
        failures-before-unavailable number> < successes-before-available number |
        send-when-unavailable < successes-before-available number>);
    transaction-timeout seconds;
}
clusters [
    cluster-name;
    server server-name {
        priority priority-level;
        weight weight-level;
    }
}
default-availability-check-profile profile-name;
}
servers {
    server-name {
        address ip4-address <port port-number> <transport (udp | tcp)>;
        admission-control profile-name;
        availability-check-profile profile-name;
        service-point service-point-name;
    }
}
timers {
    inactive-call seconds;
    timer-c seconds;
}
}
traceoptions {
    file {
        filename filename;
        files number;
        match regex;
        size size;
    }
    flag {
        datastore {
            data trace-level;
            db trace-level;
            handle trace-level;
            minimum trace-level;
        }
        framework {
            action trace-level;
            event trace-level;
            executor trace-level;
            freezer trace-level;
            minimum trace-level;
            memory-pool trace-level;
        }
    }
    minimum trace-level;
    sbc-utils {
        common trace-level;
        configuration trace-level;
        device-monitor trace-level;
        ipc trace-level;
    }
}

```

```

        memory-management trace-level;
        message trace-level;
        minimum trace-level;
        user-interface trace-level;
    }
    session-trace trace-level;
    signaling {
        b2b trace-level;
        b2b-wrapper trace-level;
        minimum trace-level;
        policy trace-level;
        sip-stack-wrapper trace-level;
        topology-hiding trace-level;
        ua trace-level;
    }
    sip-stack {
        dev-logging;
        event-tracing;
        ips-tracing;
        pd-log-detail (full | summary);
        pd-log-level (audit | exception | problem);
        per-tracing;
        verbose-logging;
    }
}
}
}
}
cos {
    application-profile profile-name {
        ftp {
            data {
                dscp (alias | bits);
                forwarding-class class-name;
            }
        }
        sip {
            video {
                dscp (alias | bits);
                forwarding-class class-name;
            }
            voice {
                dscp (alias | bits);
                forwarding-class class-name;
            }
        }
    }
}
rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
        from {
            application-sets set-name;
            applications [ application-names ];
            destination-address (CoS) address;
            destination-prefix-list list-name <except>;
            source-address address;

```

```

        source-prefix-list list-name <except>;
    }
    then {
        application-profile profile-name;
        dscp (alias | bits);
        forwarding-class class-name;
        (reflexive | reverse) {
            application-profile profile-name;
            dscp (alias | bits);
            forwarding-class class-name;
            syslog;
        }
        syslog;
    }
}
rule-set rule-set-name {
    rule rule-name;
}
}
dynamic-flow-capture {
    capture-group client-name {
        content-destination identifier {
            address address;
            hard-limit bandwidth;
            hard-limit-target bandwidth;
            soft-limit bandwidth;
            soft-limit-clear bandwidth;
            ttl hops;
        }
        control-source identifier {
            allowed-destinations [ destination ];
            minimum-priority value;
            no-syslog;
            notification-targets address port port-number;
            service-port port-number;
            shared-key value;
            source-addresses [ address ];
        }
        duplicates-dropped-periodicity seconds;
        input-packet-rate-threshold rate;
        interfaces interface-name;
        max-duplicates number;
        pic-memory-threshold percentage percentage;
    }
    g-max-duplicates number;
    g-duplicates-dropped-periodicity seconds;
}
ip-reassembly{
    profile profile-name
    rule rule-name{
        match-direction direction;
    }
}
flow-collector {
    analyzer-address address;
    analyzer-id name;
}

```

```

destinations {
  ftp:url {
    password "password";
  }
  file-specification {
    variant variant-number {
      data-format format;
      name-format format;
      transfer {
        record-level number;
        timeout seconds;
      }
    }
  }
}
interface-map {
  collector interface-name;
  file-specification variant-number;
  interface-name {
    collector interface-name;
    file-specification variant-number;
  }
}
retry number;
retry-delay seconds;
transfer-log-archive {
  archive-sites {
    ftp:url {
      password "password";
      username username;
    }
  }
  filename-prefix prefix;
  maximum-age minutes;
}
}
flow-monitoring {
  version9 {
    template template-name {
      flow-active-timeout seconds;
      flow-inactive-timeout seconds;
      ipv4-template;
      ipv6-template;
      mpls-template {
        label-position [ positions ];
      }
      mpls-ipv4-template {
        label-position [ positions ];
      }
      option-refresh-rate packets packets seconds seconds;
      template-refresh-rate packets packets seconds seconds;
    }
  }
}
}
flow-tap {
  (interface interface-name | tunnel-interface interface-name);
}

```

```

ids {
  rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
      from {
        application-sets set-name;
        applications [ application-names ];
        destination-address (address | any-unicast) <except>;
        destination-address-range low minimum-value high maximum-value <except>;
        destination-prefix-list list-name <except>;
        source-address (address | any-unicast) <except>;
        source-address-range low minimum-value high maximum-value <except>;
        source-prefix-list list-name <except>;
      }
      then {
        aggregation {
          destination-prefix prefix-number | destination-prefix-ipv6 prefix-number;
          source-prefix prefix-number | source-prefix-ipv6 prefix-number;
        }
        (force-entry | ignore-entry);
        logging {
          syslog;
          threshold rate;
        }
        session-limit {
          by-destination {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
          }
          by-pair {
            maximum number;
            packets number;
            rate number;
          }
          by-source {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
          }
        }
        syn-cookie {
          mss value;
          threshold rate;
        }
      }
    }
  }
  rule-set rule-set-name {
    rule rule-name;
  }
}
ipsec-vpn {
  clear-ike-sas-on-pic-restart;
}

```

```

clear-ipsec-sas-on-pic-restart;
ike {
  proposal proposal-name {
    authentication-algorithm (md5 | sha1 | sha-256);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group2 | group5 | group14);
    encryption-algorithm algorithm;
    lifetime-seconds seconds;
  }
  policy policy-name {
    description description;
    local-certificate identifier;
    local-id (ipv4_addr ipv4-address | ipv6_addr ipv6-address | key-id identifier);
    version (1 | 2);
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
    remote-id {
      ipv4_addr [ values ];
      ipv6_addr [ values ];
      key_id [ values ];
    }
  }
}
ipsec {
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    description description;
    encryption-algorithm algorithm;
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
  }
  policy policy-name {
    description description;
    perfect-forward-secrecy {
      keys (group1 | group2);
    }
    proposals [ proposal-names ];
  }
}
rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      destination-address address;
      ipsec-inside-interface interface-name;
      source-address address;
    }
    then {
      anti-replay-window-size bits;
      backup-remote-gateway address;
      clear-dont-fragment-bit;
      dynamic {
        ike-policy policy-name;
        ipsec-policy policy-name;
      }
    }
  }
}

```

```

    }
    initiate-dead-peer-detection;
    manual {
        direction (inbound | outbound | bidirectional) {
            authentication {
                algorithm (hmac-md5-96 | hmac-sha1-96);
                key (ascii-text key | hexadecimal key );
            }
            auxiliary-spi spi-value;
            encryption {
                algorithm algorithm;
                key (ascii-text key | hexadecimal key );
            }
            protocol (ah | bundle | esp);
            spi spi-value;
        }
    }
    no-anti-replay;
    remote-gateway address;
    syslog;
    tunnel-mtu bytes;
}
}
}
rule-set rule-set-name {
    rule rule-name;
}
no-ipsec-tunnel-in-traceroute;
traceoptions {
    file {
        files number;
        size bytes;
    }
    flag flag;
    level level;
}
}
l2tp {
    tunnel-group name {
        hello-interval seconds;
        hide-avps;
        l2tp-access-profile profile-name;
        local-gateway address;
        maximum-send-window packets;
        ppp-access-profile profile-name;
        receive-window packets;
        retransmit-interval seconds;
        service-interface interface-name;
        syslog {
            host hostname {
                services severity-level;
                facility-override facility-name;
                log-prefix prefix-value;
            }
        }
    }
}
tunnel-timeout seconds;

```

```

}
traceoptions {
  debug-level level;
  filter {
    protocol name;
  }
  flag flag;
  interfaces interface-name {
    debug-level level;
    flag flag;
  }
}
}
logging {
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>
      <match regex>;
    flag flag;
  }
}
nat {
  ipv6-multicast-interfaces (all | interface-name) {
    disable;
  }
  pool nat-pool-name {
    address ip-prefix </prefix-length>;
    address-range low minimum-value high maximum-value;
    pgcp {
      hint [ hint-strings ];
      ports-per-session ports;
      remotely-controlled;
      transport;
    }
    port (automatic | range low minimum-value high maximum-value) {
      random-allocation;
    }
  }
  rule rule-name {
    match-direction (input | output);
    term term-name {
      from {
        application-sets set-name;
        applications [ application-names ];
        destination-address (address | any-unicast) <except>;
        destination-address-range low minimum-value high maximum-value <except>;
        destination-prefix-list list-name <except>;
        source-address (address | any-unicast) <except>;
        source-address-range low minimum-value high maximum-value <except>;
        source-prefix-list list-name <except>;
      }
      then {
        syslog;
        translated {
          destination-pool nat-pool-name;
          destination-prefix destination-prefix;
          dns-alg-pool dns-alg-pool;

```

```

    dns-alg-prefix dns-alg-prefix;
    overload-pool overload-pool-name;
    overload-prefix overload-prefix;
    source-pool nat-pool-name;
    source-prefix source-prefix;
    translation-type {
        (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | dynamic-nat44 |
         napt-44 | napt-66 | napt-pt | stateful-nat64 | twice-basic-nat-44
         |twice-dynamic-nat-44 |twice-napt-44);
    }
    use-dns-map-for-destination-translation;
}
}
}
}
rule-set rule-set-name {
    rule rule-name;
}
}
pgcp {
    gateway gateway-name {
        cleanup-timeout seconds;
        gateway-address gateway-address;
        fast-update-filters {
            maximum-terms number-of-terms;
            maximum-fuf-percentage percentage;
        }
        gateway-controller gateway-controller-name {
            controller-address ip-address;
            controller-port port-number;
            interim-ah-scheme {
                algorithm algorithm;
            }
        }
    }
    gateway-port gateway-port;
    graceful-restart {
        maximum-synchronization-mismatches number-of-mismatches;
        seconds;
    }
    data-inactivity-detection {
        inactivity-delay seconds;
        latch-deadlock-delay seconds;
        send-notification-on-delay;
        inactivity-duration seconds;
        no-rtcp-check
        stop-detection-on-drop;
        report-service-change {
            service-change-type (forced-906) | forced-910;
        }
    }
}
h248-properties {
    application-data-inactivity-detection {
        ip-flow-stop-detection (regulated-notify | immediate-notify);
    }
}
base-root {
    mg-provisional-response-timer-value {

```

```
    default milliseconds;
    maximum milliseconds;
    minimum milliseconds;
  }
  mgc-originated-pending-limit {
    default number-of-messages;
    maximum number-of-messages;
    minimum number-of-messages;
  }
  normal-mg-execution-time {
    default milliseconds;
    maximum milliseconds;
    minimum milliseconds;
  }
  normal-mgc-execution-time {
    default milliseconds;
    maximum milliseconds;
    minimum milliseconds;
  }
}
diffserv {
  dscp {
    default (dscp-value | alias | do-not-change);
  }
}
event-timestamp-notification {
  request-timestamp (requested | suppressed | autonomous);
}
hanging-termination-detection {
  timerx seconds;
}
notification-behavior {
  notification-regulation default (once | 0 - 100);
}
segmentation {
  mg-segmentation-timer {
    default milliseconds;
    maximum milliseconds;
    minimum milliseconds;
  }
  mgc-segmentation-timer {
    default milliseconds;
    maximum milliseconds;
    minimum milliseconds;
  }
  mg-maximum-pdu-size {
    default bytes;
    maximum bytes;
    minimum bytes;
  }
  mgc-maximum-pdu-size {
    default bytes;
    maximum bytes;
    minimum bytes;
  }
}
```

```

traffic-management {
  max-burst-size {
    default bytes-per-second;
    maximum bytes-per-second;
    minimum bytes-per-second;
    rtcp {
      (fixed-value bytes-per-second | percentage percentage);
    }
  }
  peak-data-rate {
    default bytes-per-second;
    maximum bytes-per-second;
    minimum bytes-per-second;
    rtcp {
      (fixed-value bytes-per-second | percentage percentage);
    }
  }
  sustained-data-rate {
    default bytes-per-second;
    maximum bytes-per-second;
    minimum bytes-per-second;
    rtcp {
      (fixed-value bytes-per-second | percentage percentage);
    }
    rtcp-include;
  }
}
inactivity-timer {
  inactivity-timeout {
    detect;
    maximum-inactivity-time {
      default 10-millisecond-units;
      maximum 10-millisecond-units;
      minimum 10-millisecond-units;
    }
  }
}
}
h248-options {
  audit-observed-events-returns;
  encoding {
    no-dscp-bit-mirroring;
    use-lower-case
  }
  service-change {
    context-indications {
      state-loss (forced-910 | forced-915 | none);
    }
    control-association-indications {
      disconnect {
        controller-failure (failover-909 | restart-902);
        reconnect (disconnected-900 | restart-902);
      }
      down {
        administrative (forced-905 | forced-908 | none);
        failure (forced-904 | forced-908 | none);
      }
    }
  }
}

```

```

    graceful (graceful-905 | none);
  }
  up {
    cancel-graceful (none | restart-918);
    failover-cold (failover-920 | restart-901);
    failover-warm (failover-919 | restart-902);
  }
}
virtual-interface-indications {
  virtual-interface-down {
    administrative (forced-905 | forced-906 | none);
    failure (forced-904 | forced-906 | none);
    graceful (graceful-905 | none);
  }
  use-wildcard-response;
  virtual-interface-up {
    cancel-graceful (none | restart-918);
    warm (none | restart-900);
  }
}
}
}
h248-timers {
  initial-average-ack-delay milliseconds;
  maximum-net-propagation-delay milliseconds;
  maximum-waiting-delay milliseconds;
  tmax-retransmission-delay milliseconds;
}
max-concurrent-calls number-of-calls;
monitor {
  media {
    rtcp;
    rtp;
  }
}
service-state (in-service | out-of-service-forced | out-of-service-graceful);
session-mirroring {
  delivery-function delivery-function-name {
    destination-address destination-address;
    destination-port destination-port;
    network-operator-id network-operator-id;
    source-address source-address;
    source-port (Mirrored BGF Packets) source-port;
  }
  disable-session-mirroring;
}
}
nat-pool nat-pool-name;
rule rule-name {
  gateway gateway-name;
  nat-pool nat-pool-name;
}
rule-set rule-set-name {
  rule rule-name;
}
}
traceoptions {

```

```

file <filename filename> <files number> <match regex> <size size> <world-readable
| no-world-readable>;
flag {
  bgf-core {
    common trace-level;
    default trace-level;
    firewall trace-level;
    gate-logic trace-level;
    pic-broker trace-level;
    policy trace-level;
    statistics trace-level;
  }
  default trace-level;
  h248-stack {
    control-association trace-level;
    default trace-level;
    messages;
    media-gateway trace-level;
  }
  sbc-utils {
    common trace-level;
    configuration trace-level;
    default trace-level;
    device-monitor trace-level;
    ipc trace-level;
    memory-management trace-level;
    messaging trace-level;
    user-interface trace-level;
  }
}
}
virtual-interface interface-number {
  nat-pool nat-pool-name;
  service-interface interface-identifier;
  routing-instance instance-name {
    service-interface interface-name.unit-number;
  }
  service-state (in-service | out-of-service-forced | out-of-service-graceful);
}
session-mirroring {
  delivery-function delivery-function-name {
    destination-address destination-address;
    destination-port destination-port;
    network-operator-id network-operator-id;
    source-address source-address;
    source-port (Mirrored BGF Packets) source-port;
  }
  disable-session-mirroring;
}
}
ptsp {
  forward-rule rule-name {
    term precedence {
      from {
        application-groups [ application-group-name ];
        applications [ application-name ];
      }
    }
  }
}

```

```

        local-address address <except>;
        local-address-range low low-value high high-value <except>;
        local-prefix-list prefix-list-name <except>;
    }
    then {
        forwarding-instance forwarding-instance unit-number unit-number;
    }
}
}
rule rule-name {
    count-type (application | rule);
    demux (destination-address | source-address);
    forward-rule forward-rule-name;
    match-direction (input | input-output | output);
    term precedence {
        from {
            application-group-any;
            application-groups [ application-group-name ];
            applications [ application-name ];
            local-port-range low low-value high high-value;
            local-ports [ value-list ];
            protocol protocol-number;
            remote-address address <except>;
            remote-address-range low low-value high high-value <except>;
            remote-port-range low low-value high high-value;
            remote-ports [ value-list ];
            remote-prefix-list prefix-list-name <except>;
        }
        then {
            (accept | discard);
            count (application | application-group | application-group-any | rule | none);
            forwarding-class forwarding-class;
            police policer-name;
        }
    }
}
rule-set rule-set-name {
    rule rule-name;
}
}
rpm {
    bgp {
        data-fill data;
        data-size size;
        destination-port port;
        history-size size;
        logical-system logical-system-name <routing-instances routing-instance-name>;
        moving-average-size number;
        probe-count count;
        probe-interval seconds;
        probe-type type;
        routing-instances instance-name;
        test-interval interval;
    }
    probe owner {
        test test-name {

```

```

    data-fill data;
    data-size size;
    destination-interface interface-name;
    destination-port port;
    dscp-code-point dscp-bits;
    hardware-timestamp;
    history-size size;
    moving-average-size number;
    one-way-hardware-timestamp;
    probe-count count;
    probe-interval seconds;
    probe-type type;
    routing-instance instance-name;
    source-address address;
    target (url | address);
    test-interval interval;
    thresholds thresholds;
    traps traps;
  }
}
probe-limit limit;
probe-server {
  tcp {
    destination-interface interface-name;
    port number;
  }
  udp {
    destination-interface interface-name;
    port number;
  }
}
twamp {
  server {
    authentication-mode (authenticated | encrypted | none);
    client-list list-name {
      address address;
    }
    inactivity-timeout seconds;
    maximum-connections count;
    maximum-connections-per-client count;
    maximum-sessions count;
    maximum-sessions-per-connection count;
    port number;
  }
}
}
service-set service-set-name {
  aacl-rules rule-name;
  policy-decision-statistics-profile profile-name;
  (ids-rules rule-names | ids-rule-sets rule-set-name);
  (ipsec-vpn-rules rule-names | ipsec-vpn-rule-sets rule-set-name);
  (nat-rules rule-names | nat-rule-sets rule-set-name);
  (pgcp-rules rule-names | pgcp-rule-sets rule-set-name);
  (ptsp-rules rule-names | ptsp-rule-sets rule-set-name);
  (stateful-firewall-rules rule-names | stateful-firewall-rule-sets rule-set-name);
  allow-multicast;
}

```

```

extension-service service-name {
    provider-specific rules;
}
interface-service {
    service-interface interface-name;
}
ip-reassembly-rules
ipsec-vpn-options {
    anti-replay-window-size bits;
    clear-dont-fragment-bit;
    ike-access-profile profile-name;
    local-gateway address;
    no-anti-replay;
    passive-mode-tunneling;
    trusted-ca [ ca-profile-names ];
    tunnel-mtu bytes;
}
max-flows number;
next-hop-service {
    inside-service-interface interface-name.unit-number;
    outside-service-interface interface-name.unit-number;
    outside-service-interface-type interface-type;
    service-interface-pool name;
}
service-order {
    forward-flow [ service-name1 service-name2 ];
    reverse-flow [ service-name1 service-name2 ];
}
syslog {
    host hostname {
        services severity-level;
        facility-override facility-name;
        port port-number;
    }
}
}
software {
    software-concentrator {
        ds-lite ds-lite-software-concentrator {
            auto-update-mtu;
            copy-dscp;
            flow-limit flow-limit;
            mtu-v6 mtu-v6;
            software-address address;
        }
        v6rd v6rd-software-concentrator {
            ipv4-prefix ipv4-prefix;
            v6rd-prefix ipv6-prefix;
            mtu-v4 mtu-v4;
        }
    }
}
rule rule-name {
    match-direction (input | output);
    term term-name {
        then {
            ds-lite name;

```

```

    }
  }
}
ipv6-multicast-filters
}
stateful-firewall {
  rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
      from {
        application-sets set-name;
        applications [ application-names ];
        destination-address (address | any-unicast) <except>;
        destination-address-range low minimum-value high maximum-value <except>;
        destination-prefix-list list-name <except>;
        source-address (address | any-unicast) <except>;
        source-address-range low minimum-value high maximum-value <except>;
        source-prefix-list list-name <except>;
      }
      then {
        (accept | discard | reject);
        allow-ip-options [ values ];
        syslog;
      }
    }
  }
}
rule-set rule-set-name {
  rule rule-name;
}
}
}

```



## PART 2

# Adaptive Services

- [Adaptive Services Overview on page 39](#)
- [Applications Configuration Guidelines on page 125](#)
- [Summary of Applications Configuration Statements on page 179](#)
- [Network Address Translation Configuration Guidelines on page 191](#)
- [Summary of Network Address Translation Configuration Statements on page 305](#)
- [Softwire Configuration Guidelines on page 343](#)
- [Summary of Softwire Services Configuration Statements on page 367](#)
- [Network Address Translation and Softwire Administration on page 373](#)
- [Stateful Firewall Services Configuration Guidelines on page 387](#)
- [Summary of Stateful Firewall Configuration Statements on page 397](#)
- [Stateful Firewall on the Embedded Junos OS Platform Configuration Guidelines on page 409](#)
- [Summary of Stateful Firewall on the Embedded Junos OS Platform Configuration Statements on page 413](#)
- [Load Balancing Configuration Guidelines on page 425](#)
- [Summary of Load Balancing Configuration Statements on page 431](#)
- [Intrusion Detection Service Configuration Guidelines on page 445](#)
- [Summary of Intrusion Detection Service Configuration Statements on page 457](#)
- [IPsec Services Configuration Guidelines on page 479](#)
- [Summary of IPsec Services Configuration Statements on page 535](#)
- [Layer 2 Tunneling Protocol Services Configuration Guidelines on page 577](#)
- [Summary of Layer 2 Tunneling Protocol Configuration Statements on page 597](#)
- [Link Services IQ Interfaces Configuration Guidelines on page 615](#)
- [Summary of Link Services IQ Configuration Statements on page 681](#)
- [Voice Services Configuration Guidelines on page 695](#)
- [Summary of Voice Services Configuration Statements on page 705](#)
- [Class-of-Service Configuration Guidelines on page 715](#)
- [Summary of Class-of-Service Configuration Statements on page 725](#)
- [Service Set Configuration Guidelines on page 741](#)

- [Summary of Service Set Configuration Statements on page 761](#)
- [Service Interface Configuration Guidelines on page 795](#)
- [Summary of Service Interface Configuration Statements on page 813](#)
- [PGCP Configuration Guidelines for the BGF Feature on page 837](#)
- [Summary of PGCP Configuration Statements on page 843](#)
- [Service Interface Pools Configuration Guidelines on page 949](#)
- [Summary of Service Interface Pools Statements on page 951](#)
- [PTSP Configuration Guidelines on page 953](#)
- [Summary of PTSP Configuration Statements on page 955](#)

## CHAPTER 3

# Adaptive Services Overview

This chapter discusses the following topics:

- [Adaptive Services Overview on page 39](#)
- [Enabling Service Packages on page 41](#)
- [Services Configuration Procedure on page 46](#)
- [Packet Flow Through the Adaptive Services or Multiservices PIC on page 47](#)
- [Junos Network Secure Overview on page 48](#)
- [Junos Address Aware Network Addressing Overview on page 51](#)
- [Sample IPv6 Transition Scenarios on page 52](#)
- [Junos OS CGNAT Implementation Overview on page 53](#)
- [Port Control Protocol Overview on page 64](#)
- [Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card on page 66](#)
- [ALGs Available by Default for Junos OS Address Aware NAT on page 69](#)
- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 71](#)
- [Understanding Junos VPN Site Secure on page 75](#)
- [Layer 2 Tunneling Protocol Overview on page 78](#)
- [Voice Services Overview on page 79](#)
- [HTTP URL Tracking and Policy Control for Client Requests on page 79](#)
- [Configuring HTTP URL Tracking and Policy Control on page 81](#)
- [Class of Service Overview on page 82](#)
- [Configuring Routing Services on Multiservices MIC and MPC \(MS-MIC and MS-MPC\) on page 82](#)
- [Examples: Services Interfaces Configuration on page 117](#)

## Adaptive Services Overview

---

MultiServices PICs and MultiServices Dense Port Concentrators (MS-DPCs) provide *adaptive services interfaces*, which allow you to coordinate multiple services on a single PIC by configuring a set of services and applications. MultiServices PICs and MS-DPCs offer a special range of services you configure in one or more service sets.

The MultiServices PIC is available in three versions, the MultiServices 100, the MultiServices 400, and the MultiServices 500, which differ in memory size and performance. All versions offer enhanced performance in comparison with AS PICs. MultiServices PICs are supported on M Series and T Series routers except M20 routers.

The MultiServices DPC is available for MX Series routers; it includes a subset of the functionality supported on the MultiServices PIC. Currently the MultiServices DPC supports the following Layer 3 services: stateful firewall, NAT, IDS, IPsec, active flow monitoring, RPM, and generic routing encapsulation (GRE) tunnels (including GRE key and fragmentation); it also supports graceful Routing Engine switchover (GRES) and Dynamic Application Awareness for Junos OS. For more information about supported packages, see [“Enabling Service Packages” on page 41](#).

It is also possible to group several Multiservices PICs into an aggregated Multiservices (AMS) system. An AMS configuration eliminates the need for separate routers within a system. The primary benefit of having an AMS configuration is the ability to support load balancing of traffic across multiple services PICs. Starting with Junos OS 11.4, all MX Series routers will support high availability (HA) and Network Address Translation (NAT) on AMS infrastructure. See [“Configuring Load Balancing on AMS Infrastructure” on page 425](#) for more information.



**NOTE:** The MultiServices PICs are polling based and not interrupt based; as a result, a high value in the `show chassis pic` “Interrupt load average” field may not mean that the PIC has reached its maximum limit of processing.

---

The following services are configured within a service set and are available only on adaptive services interfaces:

- Stateful firewall—A type of firewall filter that considers state information derived from previous communications and other applications when evaluating traffic.
- Network Address Translation (NAT)—A security procedure for concealing host addresses on a private network behind a pool of public addresses.
- Intrusion detection service (IDS)—A set of tools for detecting, redirecting, and preventing certain kinds of network attack and intrusion.
- IP Security (IPsec)—A set of tools for configuring manual or dynamic security associations (SAs) for encryption of data traffic.
- Class of service (CoS)—A subset of CoS functionality for services interfaces, limited to DiffServ code point (DSCP) marking and forwarding-class assignment. CoS BA classification is not supported on services interfaces.

The configuration for these services comprises a series of rules that you can arrange in order of precedence as a *rule set*. Each rule follows the structure of a firewall filter, with a **from** statement containing input or match conditions and a **then** statement containing actions to be taken if the match conditions are met.

The following services are also configured on the MultiServices PICs and MS-DPCs, but do not use the rule set definition:

- Layer 2 Tunneling Protocol (L2TP)—A tool for setting up secure tunnels using Point-to-Point Protocol (PPP) encapsulation across Layer 2 networks.
- Link Services Intelligent Queuing (LSQ)—Interfaces that support Junos OS class-of-service (CoS) components, link fragmentation and interleaving (LFI) (FRF.12), Multilink Frame Relay (MLFR) user-to-network interface (UNI) network-to-network interface (NNI) (FRF.16), and Multilink PPP (MLPPP).
- Voice services—A feature that uses the Compressed Real-Time Transport Protocol (CRTP) to enable voice over IP traffic to use low-speed links more effectively.

In addition, Junos OS includes the following tools for configuring services:

- Application protocols definition—Allows you to configure properties of application protocols that are subject to processing by router services, and group the application definitions into application sets.
- Service-set definition—Allows you to configure combinations of directional rules and default settings that control the behavior of each service in the service set.



**NOTE:** Logging of adaptive services interfaces messages to an external server by means of the fxp0 port is not supported on M Series routers. The architecture does not support system logging traffic out of a management interface. Instead, access to an external server is supported on a Packet Forwarding Engine interface.

#### Related Documentation

- [Understanding Services PICs on page 3](#)
- [Packet Flow Through the Adaptive Services or Multiservices PIC on page 47](#)
- [Enabling Service Packages on page 41](#)
- [Services Configuration Procedure on page 46](#)
- [Supported Platforms on page 5](#)

## Enabling Service Packages

For AS PICs, Multiservices PICs, Multiservices DPCs, and the internal Adaptive Services Module (ASM) in the M7i router, there are two service packages: Layer 2 and Layer 3. Both service packages are supported on all adaptive services interfaces, but you can enable only one service package per PIC, with the exception of a combined package supported on the ASM. On a single router, you can enable both service packages by installing two or more PICs on the platform.



**NOTE:** Graceful Routing Engine switchover (GRES) is automatically enabled on all services PICs and DPCs except the ES PIC. It is supported on all M Series, MX Series, and T Series routers except for TX Matrix routers. Layer 3 services should retain state after switchover, but Layer 2 services will restart. For IPsec services, Internet Key Exchange (IKE) negotiations are not stored and must be restarted after switchover. For more information about GRES, see the *Junos OS High Availability Library for Routing Devices*.

You enable service packages per PIC, not per port. For example, if you configure the Layer 2 service package, the entire PIC uses the configured package. To enable a service package, include the service-package statement at the `[edit chassis fpc slot-number pic pic-number adaptive-services]` hierarchy level, and specify `layer-2` or `layer-3`:

```
[edit chassis fpc slot-number pic pic-number adaptive-services]
service-package (layer-2 | layer-3);
```

To determine which package an AS PIC supports, issue the `show chassis hardware` command: if the PIC supports the Layer 2 package, it is listed as **Link Services II**, and if it supports the Layer 3 package, it is listed as **Adaptive Services II**. To determine which package a Multiservices PIC supports, issue the `show chassis pic fpc-slot slot-number pic-slot slot-number` command. The **Package** field displays the value **Layer-2** or **Layer-3**.



**NOTE:** The ASM has a default option (`layer-2-3`) that combines the features available in the Layer 2 and Layer 3 service packages.

After you commit a change in the service package, the PIC is taken offline and then brought back online immediately. You do not need to manually take the PIC offline and online.



**NOTE:** Changing the service package causes all state information associated with the previous service package to be lost. You should change the service package only when there is no active traffic going to the PIC.

The services supported in each package differ by PIC and platform type.

[Table 3 on page 43](#) lists the services supported within each service package for each PIC and platform. For information about services supported on SRX Series Services Gateways and J Series Services Routers, see the *Junos OS Feature Support Reference for SRX Series and J Series Devices*.

On the AS and Multiservices PICs, *link services* support includes Junos OS CoS components, LFI (FRF.12), MLFR end-to-end (FRF.15), MLFR UNI NNI (FRF.16), MLPPP (RFC 1990), and multiclass MLPPP. For more information, see [“Layer 2 Service Package Capabilities and Interfaces” on page 45](#) and [“Layer 2 Service Package Capabilities and Interfaces” on page 616](#).



**NOTE:** The AS PIC II for Layer 2 Service is dedicated to supporting the Layer 2 service package only.

For additional information about Layer 3 services, see the *Junos OS, Release 14.1*.

**Table 3: AS and Multiservices PIC Services by Service Package, PIC, and Platform**

Services	ASM	AS/AS2 PICs and Multiservices PICs	AS/AS2 and Multiservices PICs	AS2 and Multiservices PICs	AS2 and Multiservices PICs
Layer 2 Service Package (Only)	M7i	M7i, M10i, and M20	M40e and M120	M320, T320, and T640	TX Matrix
Link Services:					
• Link services	Yes	Yes	Yes	Yes	No
• Multiclass MLPPP	Yes	Yes	Yes	Yes	No
Voice Services:					
• CRTP and LFI	Yes	Yes	Yes	Yes	No
• CRTP and MLPPP	Yes	Yes	Yes	Yes	No
• CRTP over PPP (without MLPPP)	Yes	Yes	Yes	Yes	No
Layer 3 Service Package (Only)	M7i	M7i, M10i, and M20	M40e and M120	M320, T320, and T640	TX Matrix
Security Services:					
• CoS	Yes	Yes	Yes	Yes	No
• Intrusion detection system (IDS)	Yes	Yes	Yes	Yes	No
• IPsec	Yes	Yes	Yes	Yes	No
• NAT	Yes	Yes	Yes	Yes	No
• Stateful firewall	Yes	Yes	Yes	Yes	No
Accounting Services:					
• Active monitoring	Yes	Yes	Yes	Yes	Yes
• Dynamic flow capture (Multiservices 400 PIC only)	No	No	No	Yes	No

Table 3: AS and Multiservices PIC Services by Service Package, PIC, and Platform (*continued*)

Services	ASM	AS/AS2 PICs and Multiservices PICs	AS/AS2 and Multiservices PICs	AS2 and Multiservices PICs	AS2 and Multiservices PICs
• Flow-tap	Yes	Yes	Yes (M40e only)	Yes	No
• Passive monitoring (Multiservices 400 PIC only)	No	Yes	Yes (M40e only)	Yes	No
• Port mirroring	Yes	Yes	Yes	Yes	Yes
LNS Services:					
• L2TP LNS	Yes	Yes (M7i and M10i only)	Yes (M120 only)	No	No
Voice Services:					
• BGF	Yes	Yes	Yes	Yes	No
Layer 2 and Layer 3 Service Package (Common Features)	M7i	M7i, M10i, and M20	M40e and M120	M320, T320, and T640	TX Matrix
RPM Services:					
• RPM probe timestamping	Yes	Yes	Yes	Yes	No
Tunnel Services:					
• GRE ( <i>gr-fpc/pic/port</i> )	Yes	Yes	Yes	Yes	Yes
• GRE fragmentation ( <i>clear-dont-fragment-bit</i> )	Yes	Yes	Yes	No	No
• GRE key	Yes	Yes	Yes	Yes	No
• IP-IP tunnels ( <i>ip-fpc/pic/port</i> )	Yes	Yes	Yes	Yes	Yes
• Logical tunnels ( <i>lt-fpc/pic/port</i> )	No	No	No	No	No
• Multicast tunnels ( <i>mt-fpc/pic/port</i> )	Yes	Yes	Yes	Yes	Yes
• PIM de-encapsulation ( <i>pd-fpc/pic/port</i> )	Yes	Yes	Yes	Yes	Yes
• PIM encapsulation ( <i>pe-fpc/pic/port</i> )	Yes	Yes	Yes	Yes	Yes
• Virtual tunnels ( <i>vt-fpc/pic/port</i> )	Yes	Yes	Yes	Yes	Yes

## Layer 2 Service Package Capabilities and Interfaces

When you enable the Layer 2 service package, you can configure link services. On the AS and Multiservices PICs and the ASM, link services include support for the following:

- Junos CoS components—“[Layer 2 Service Package Capabilities and Interfaces](#)” on [page 616](#) describes how the Junos CoS components work on link services IQ (**lsq**) interfaces. For detailed information about Junos CoS components, see the *Junos OS Class of Service Library for Routing Devices*.
- LFI on Frame Relay links using FRF.12 end-to-end fragmentation—The standard for FRF.12 is defined in the specification FRF.12, *Frame Relay Fragmentation Implementation Agreement*.
- LFI on MLPPP links.
- MLFR UNI NNI (FRF.16)—The standard for FRF.16 is defined in the specification FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*.
- MLPPP (RFC 1990)
- MLFR end-to-end (FRF.15)

For the LSQ interface on the AS and Multiservices PICs, the configuration syntax is almost the same as for Multilink and Link Services PICs. The primary difference is the use of the interface-type descriptor **lsq** instead of **ml** or **ls**. When you enable the Layer 2 service package, the following interfaces are automatically created:

```
gr-fpc/pic/port
ip-fpc/pic/port
lsq-fpc/pic/port
lsq-fpc/pic/port:0
...
lsq-fpc/pic/port:N
mt-fpc/pic/port
pd-fpc/pic/port
pe-fpc/pic/port
sp-fpc/pic/port
vt-fpc/pic/port
```

Interface types **gr**, **ip**, **mt**, **pd**, **pe**, and **vt** are standard tunnel interfaces that are available on the AS and Multiservices PICs whether you enable the Layer 2 or the Layer 3 service package. These tunnel interfaces function the same way for both service packages, except that the Layer 2 service package does not support some tunnel functions, as shown in [Table 3 on page 43](#).

Interface type **lsq-fpc/pic/port** is the physical link services IQ (**lsq**) interface. Interface types **lsq-fpc/pic/port:0** through **lsq-fpc/pic/port:N** represent FRF.16 bundles. These interface types are created when you include the **mlfr-uni-nni-bundles** statement at the **[edit chassis fpc slot-number pic pic-number]** option. For more information, see “[Layer 2 Service Package Capabilities and Interfaces](#)” on [page 616](#) and *Link and Multilink Properties*.



**NOTE:** Interface type **sp** is created because it is needed by the Junos OS. For the Layer 2 service package, the **sp** interface is not configurable, but you should not disable it.

**Related  
Documentation**

- [Understanding Services PICs on page 3](#)
- [Adaptive Services Overview on page 39](#)
- [Supported Platforms on page 5](#)
- [Packet Flow Through the Adaptive Services or Multiservices PIC on page 47](#)
- [Services Configuration Procedure on page 46](#)

---

## Services Configuration Procedure

You follow these general steps to configure services:

1. Define application objects by configuring statements at the **[edit applications]** hierarchy level.
2. Define service rules by configuring statements at the **[edit services (ids | ipsec-vpn | nat | stateful-firewall) rule]** hierarchy level.
3. Group the service rules by configuring the **rule-set** statement at the **[edit services (ids | ipsec-vpn | nat | stateful-firewall)]** hierarchy level.
4. Group service rule sets under a service-set definition by configuring the **service-set** statement at the **[edit services]** hierarchy level.
5. Apply the service set on an interface by including the **service-set** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service (input | output)]** hierarchy level. Alternatively, you can configure logical interfaces as a next-hop destination by including the **next-hop-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level.



**NOTE:** You can configure IDS, NAT, and stateful firewall service rules within the same service set. You must configure IPsec services in a separate service set, although you can apply both service sets to the same PIC.

**Related  
Documentation**

- [Understanding Services PICs on page 3](#)
- [Enabling Service Packages on page 41](#)
- [Supported Platforms on page 5](#)

---

## Packet Flow Through the Adaptive Services or Multiservices PIC

---

You can optionally configure service sets to be applied at one of the following three points while the packets transit the router:

- An interface service set applied at the inbound interface.
- A next-hop service set applied at the forwarding table.
- An interface service set applied at the outbound interface.

The packet flow is as follows, graphically displayed in [Figure 1 on page 48](#). (You can configure a service set as either an interface service set or a next-hop service set.)

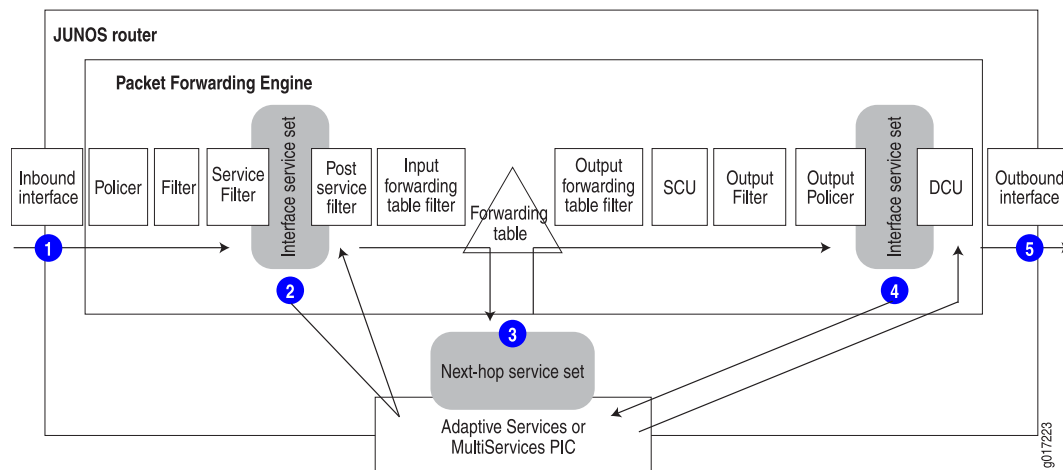
1. Packets enter the router on the inbound interface.
2. A policer, filter, service filter, service set, postservice filter, and input forwarding-table filter are applied sequentially to the traffic; these are all optional items in the configuration. If an interface service set is applied, the packets are forwarded to the AS or MultiServices PIC for services processing and then sent back to the Packet Forwarding Engine; if a service filter is also applied, only packets matching the service filter are sent to the PIC. The optional postservice filter is applied and postprocessing takes place.
3. A next-hop service set can be applied to the VPN routing and forwarding (VRF) table or to **inet.0**. If it is applied, packets are sent to the PIC for services processing and sent back to the Packet Forwarding Engine.



**NOTE:** For NAT, the next-hop service set can only be applied to the VRF table. For all other services, the next-hop service set can be applied to either the VRF table or to **inet.0**.

4. On the output interface, an output filter, output policer, and interface service set can be applied sequentially to the traffic if you have configured any of these items. If an interface service set is applied, the traffic is forwarded to the PIC for processing and sent back to the Packet Forwarding Engine, which then forwards the traffic.
5. Packets exit the router.

Figure 1: Packet Flow Through the Adaptive Services or MultiServices PIC



**NOTE:** When an AS PIC experiences persistent back pressure as a result of high traffic volume for 3 seconds, the condition triggers an automatic core dump and reboot of the PIC to help clear the blockage. A system log message at level LOG\_ERR is generated. This mechanism applies to both Layer 2 and Layer 3 service packages.

#### Related Documentation

- [Understanding Services PICs on page 3](#)
- [Adaptive Services Overview on page 39](#)
- [Supported Platforms on page 5](#)
- [Services Configuration Procedure on page 46](#)

## Junos Network Secure Overview

Routers use firewalls to track and control the flow of traffic. The following platforms employ a type of firewall called a *stateful firewall*.

- MultiServices Dense Port Concentrators (MS-DPCs)
- MS-100, MS-400, and MS-500 MultiServices PICs
- MultiServices Modular Port Concentrators (MS-MPCs), and Multiservices Modular Interface Cards (MS-MICs)

The stateful firewall capabilities provided by the Junos OS are collectively known as *Junos Network Secure*.

Contrasted with a *stateless* firewall that inspects packets in isolation, a stateful firewall provides an extra layer of security by using state information derived from past communications and other applications to make dynamic control decisions for new communication attempts. .

Stateful firewalls group relevant *flows* into *conversations*. A flow is identified by the following five properties:

- Source address
- Source port
- Destination address
- Destination port
- Protocol

A typical Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) conversation consists of two flows: the initiation flow and the responder flow. However, some conversations, such as an FTP conversation, might consist of two control flows and many data flows.

Firewall rules govern whether the conversation is allowed to be established. If a conversation is allowed, all flows within the conversation are permitted, including flows that are created during the life cycle of the conversation.

You configure stateful firewalls using a powerful rule-driven conversation handling path. A *rule* consists of direction, source address, source port, destination address, destination port, IP protocol value, and application protocol or service. In addition to the specific values you configure, you can assign the value **any** to rule objects, addresses, or ports, which allows them to match any input value. Finally, you can optionally negate the rule objects, which negates the result of the type-specific match.

Firewall rules are directional. For each new conversation, the router software checks the initiation flow matching the direction specified by the rule.

Firewall rules are ordered. The software checks the rules in the order in which you include them in the configuration. The first time the firewall discovers a match, the router implements the action specified by that rule. Rules still unchecked are ignored.



**NOTE:** MS-MPC and MS-MIC interface cards do not currently support IPv6 traffic for Junos Network Secure Stateful Firewall.

For more information, see [“Configuring Stateful Firewall Rules” on page 388](#).

## Stateful Firewall Support for Application Protocols

By inspecting the application protocol data, the Junos Network Secure stateful firewall can intelligently enforce security policies and allow only the minimal required packet traffic to flow through the firewall.

The firewall rules are configured in relation to an interface. By default, the stateful firewall allows all sessions initiated from the hosts behind the interface to pass through the router.

## Stateful Firewall Anomaly Checking

The stateful firewall recognizes the following events as anomalies and sends them to the IDS software for processing:

- IP anomalies:
  - IP version is not correct.
  - IP header length field is too small.
  - IP header length is set larger than the entire packet.
  - Bad header checksum.
  - IP total length field is shorter than header length.
  - Packet has incorrect IP options.
  - Internet Control Message Protocol (ICMP) packet length error.
  - Time-to-live (TTL) equals 0.
- IP address anomalies:
  - IP packet source is a broadcast or multicast.
  - Land attack (source IP equals destination IP).
- IP fragmentation anomalies:
  - IP fragment overlap.
  - IP fragment missed.
  - IP fragment length error.
  - IP packet length is more than 64 kilobytes (KB).
  - Tiny fragment attack.
- TCP anomalies:
  - TCP port 0.
  - TCP sequence number 0 and flags 0.
  - TCP sequence number 0 and FIN/PSH/RST flags set.
  - TCP flags with wrong combination (TCP FIN/RST or SYN/(URG|FIN|RST)).
  - Bad TCP checksum.
- UDP anomalies:
  - UDP source or destination port 0.
  - UDP header length check failed.
  - Bad UDP checksum.
- Anomalies found through stateful TCP or UDP checks:

- SYN followed by SYN-ACK packets without ACK from initiator.
- SYN followed by RST packets.
- SYN without SYN-ACK.
- Non-SYN first flow packet.
- ICMP unreachable errors for SYN packets.
- ICMP unreachable errors for UDP packets.
- Packets dropped according to stateful firewall rules.

If you employ stateful anomaly detection in conjunction with stateless detection, IDS can provide early warning for a wide range of attacks, including these:

- TCP or UDP network probes and port scanning
- SYN flood attacks
- IP fragmentation-based attacks such as teardrop, bonk, and boink

---

## Junos Address Aware Network Addressing Overview

---

In early 2011, the Internet Assigned Numbers Authority (IANA) allocated the last large block of IPv4 addresses. Now service providers and large enterprises, as well as cloud providers, e-tailers, and federal agencies, are evaluating technologies to help them avoid IPv4 address exhaustion and ensure uninterrupted subscriber and service growth.

*Junos Address Aware Network Addressing* is Juniper Networks' portfolio of IPv4 exhaustion avoidance, IPv4-IPv6 coexistence, and IPv6 transition technologies that include IPv6, v4/v6 dual stack, NAT44, NAT44(4), NAPT44, NAPT444, NAT-PT, NAT64, 6-to4-PMT, 6rd, and DS-Lite. These technologies help network operators improve subscriber and service scale, mitigate IPv4 address depletion, and pragmatically transition to IPv6 based on business requirements.

*Junos Address Aware Network Addressing* technologies are available on the following platforms:

- MultiServices Dense Port Concentrator (MS-DPC)
- MS-100, MS-400, and MS-500 MultiServices PICS
- MultiServices Modular Port Concentrator (MS-MPC) and MultiServices Modular Interface Card (MS-MIC)
- Modular Port Concentrator Types 1, 2, and 3 (inline NAT).

## Sample IPv6 Transition Scenarios

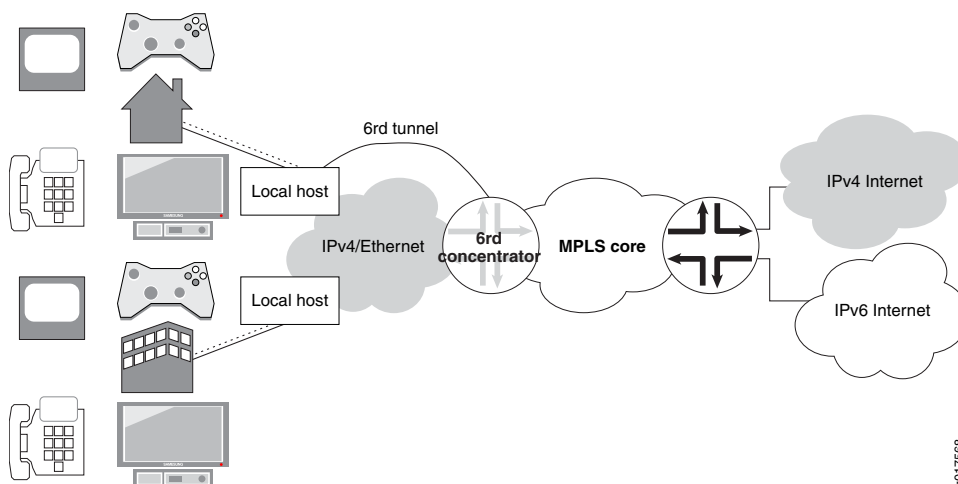
The Junos OS supports many IPv6 transition scenarios required by Junos OS customers. The following are selected examples:

- [Example 1: IPv4 Depletion with a Non-IPv6 Access Network on page 52](#)
- [Example 2: IPv4 Depletion with an IPv6 Access Network on page 52](#)
- [Example 3: IPv4 Depletion for Mobile Networks on page 53](#)

### Example 1: IPv4 Depletion with a Non-IPv6 Access Network

[Figure 2 on page 52](#) depicts a scenario in which the Internet service provider (ISP) has not significantly changed its IPv4 network. This approach enables IPv4 hosts to access the IPv4 Internet and IPv6 hosts to access the IPv6 Internet. A dual-stack host can be treated as an IPv4 host when it uses the IPv4 access service, and as an IPv6 host when it uses the IPv6 access service.

**Figure 2: IPv4 Depletion Solution - IPv4 Access Network**

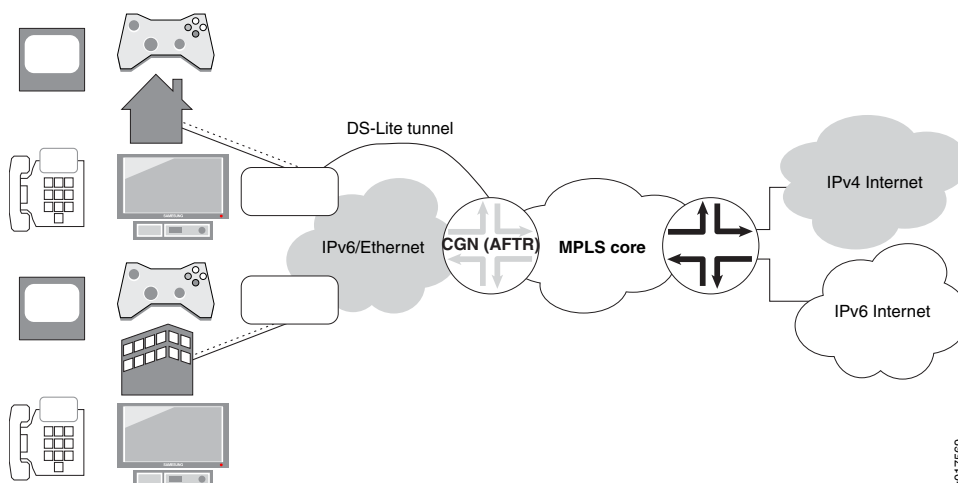


Two new types of devices must be deployed in this approach: a dual-stack home gateway and a dual-stack carrier-grade Network Address Translation (NAT). The dual-stack home gateway integrates IPv4 forwarding and v6-over-v4 tunneling functions. It can also integrate a v4-v4 NAT function. The dual-stack carrier-grade NAT (CGN) integrates v6-over-v4 tunneling and carrier-grade v4-v4 NAT functions.

### Example 2: IPv4 Depletion with an IPv6 Access Network

In the scenario shown in [Figure 3 on page 53](#), the ISP network is IPv6-only.

Figure 3: IPv4 Depletion Solution - IPv6 Access Network



The dual-stack lite (DS-Lite) solution accommodates IPv6-only ISPs. The best business model for this approach is that the customer premises equipment (CPE) has integrated the functions for tunneling IPv6 to an IPv4 backbone, tunneling IPv4 to an IPv6 backbone, and can automatically detect which solution is required.

Not all customers of a given ISP must switch from IPv4 access to IPv6 access simultaneously; in fact, transition can be managed better by switching groups of customers (for example, all those connected to a single point of presence) on an incremental basis. Such an incremental approach should prove easier to plan, schedule, and execute than an across-the-board conversion.

### Example 3: IPv4 Depletion for Mobile Networks

The complexity of mobile networks necessitates a flexible migration approach to ensure minimal disruption and maximum backward compatibility during transition. NAT64 can be used to enable IPv6 devices to communicate to IPv4 hosts without modifying the clients.

### Junos OS CGNAT Implementation Overview

The Junos OS enables its users to implement and scale their CGNAT (Carrier-Grade Network Address Translation) solutions based on the type of services interfaces used for the implementation.

- MultiServices Denser Port Concentrator (MS-DPC)—The layer 3 services package is used to configure NAT for MS-DPC adaptive services PICs. You must configure the layer-3 services package before implementing NAT on the MS-DPC. This solution provides NAT functionality described in [“Network Address Translation Overview for MS-DPC, MS-MPC, and MS-MIC Line Cards”](#) on page 54.
- MultiServices Modular Port Concentrator (MS-MPC) and MultiServices Modular Interface Card (MS-MIC)—MS-MPCs and MS-MICs are pre-configured to enable configuration of carrier-grade NAT. This solution provides NAT functionality also

described in [“Network Address Translation Overview for MS-DPC, MS-MPC, and MS-MIC Line Cards”](#) on page 54.

- [Inline NAT for Type 1, 2, and 3 Modular Port Concentrator \(MPC Line Cards\)—Inline NAT leverages the services capabilities of TRIO-based MPC line cards, allowing cost-effective implementation NAT functionality on the data plane, as described in “Inline Network Address Translation Overview for MPC Types 1, 2, and 3” on page 59](#)
- [Network Address Translation Overview for MS-DPC, MS-MPC, and MS-MIC Line Cards](#) on page 54
- [Inline Network Address Translation Overview for MPC Types 1, 2, and 3](#) on page 59
- [Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card](#) on page 60
- [ALGs Available by Default for Junos OS Address Aware NAT](#) on page 62

## Network Address Translation Overview for MS-DPC, MS-MPC, and MS-MIC Line Cards

- [Types of NAT](#) on page 54

---

### Types of NAT

The types of Network Address Translation (NAT) supported by the Junos OS are described in the following sections:

- [NAT Concept and Facilities Overview](#) on page 54
- [IPv4-to-IPv4 Basic NAT](#) on page 55
- [Static Destination NAT](#) on page 56
- [Twice NAT](#) on page 56
- [IPv6 NAT](#) on page 57
- [Application-level gateway \(ALG\) Support](#) on page 57
- [NAT-PT with DNS ALG](#) on page 57
- [Dynamic NAT](#) on page 57
- [Stateful NAT64](#) on page 58
- [Dual-Stack Lite](#) on page 58

### ***NAT Concept and Facilities Overview***

NAT is a mechanism for translating IP addresses. NAT provides the technology used to support a wide range of networking goals, including:

- Concealing a set of host addresses on a private network behind a pool of public addresses.
- Providing a security measure to protect the host addresses from direct targeting in network attacks.
- Providing a tool set for coping with IPv4 address depletion and IPV6 transition issues.

The Junos OS provides carrier-grade NAT (CGN) for IPv4 and IPv6 networks, and facilitates the transit of traffic between different types of networks.



**NOTE:** The Junos OS supports a diverse set of NAT translation options. Not all types of NAT are supported on all interface types. See [“Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card”](#) on page 60, which lists features available on supported interfaces.

- Static-source translation—Allows you to hide a private network. It features a one-to-one mapping between the original address and the translated address; the mapping is configured statically. For more information, see [“Basic NAT”](#) on page 56.
- Dynamic-source translation—Includes two options: dynamic address-only source translation and Network Address Port Translation (NAPT):
  - Dynamic address-only source translation—A NAT address is picked up dynamically from a source NAT pool and the mapping from the original source address to the translated address is maintained as long as there is at least one active flow that uses this mapping. For more information, see [“Dynamic NAT”](#) on page 57.
  - NAPT—Both the original source address and the source port are translated. The translated address and port are picked up from the corresponding NAT pool. For more information, see [“NAPT”](#) on page 56.
- Static destination translation—Allows you to make selected private servers accessible. It features a one-to-one mapping between the translated address and the destination address; the mapping is configured statically. For more information, see [“Static Destination NAT”](#) on page 56.
- Protocol translation—Allows you to assign addresses from a pool on a static or dynamic basis as sessions are initiated across IPv4 or IPv6 boundaries. For more information, see [“Configuring Protocol Translation Between IPv6 and IPv4 Networks - NAT-PT”](#) on page 240, [“NAT-PT with DNS ALG”](#) on page 57, and [“Stateful NAT64”](#) on page 58.
- Encapsulation of IPv4 packets into IPv6 packets using softwires—Enables packets to travel over softwires to a carrier-grade NAT endpoint where they undergo source-NAT processing to hide the original source address. For more information, see [“Tunneling Services for IPv4-to-IPv6 Transition Overview”](#) on page 71.

The Junos OS supports NAT functionality described in IETF RFCs and Internet drafts, as shown in *“Supported NAT and SIP Standards”* in *Standards Reference*.

#### **IPv4-to-IPv4 Basic NAT**

Basic Network Address Translation or Basic NAT is a method by which IP addresses are mapped from one group to another, transparent to end users. Network Address Port Translation or NAPT is a method by which many network addresses and their TCP/UDP ports are translated into a single network address and its TCP/UDP ports. Together, these two operations, referred to as traditional NAT, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses.

Traditional NAT, specified in RFC 3022, *Traditional IP Network Address Translator*, is fully supported by the Junos OS. In addition, NAPT is supported for source addresses.

**Basic NAT**

With Basic NAT, a block of external addresses is set aside for translating addresses of hosts in a private domain as they originate sessions to the external domain. For packets outbound from the private network, Basic NAT translates source IP addresses and related fields such as IP, TCP, UDP, and ICMP header checksums. For inbound packets, Basic NAT translates the destination IP address and the checksums listed above.

**NAPT**

Use NAPT to enable the components of the private network to share a single external address. NAPT translates the transport identifier (for example, TCP port number, UDP port number, or ICMP query ID) of the private network into a single external address. NAPT can be combined with Basic NAT to use a pool of external addresses in conjunction with port translation.

For packets outbound from the private network, NAPT translates the source IP address, source transport identifier (TCP/UDP port or ICMP query ID), and related fields, such as IP, TCP, UDP, and ICMP header checksums. For inbound packets, NAPT translates the destination IP address, the destination transport identifier, and the IP and transport header checksums.

**Static Destination NAT**

Use static destination NAT to translate the destination address for external traffic to an address specified in a destination pool. The destination pool contains one address and no port configuration.

For more information about static destination NAT, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

**Twice NAT**

In Twice NAT, both the source and destination addresses are subject to translation as packets traverse the NAT router. The source information to be translated can be either address only or address and port. For example, you would use Twice NAT when you are connecting two networks in which all or some addresses in one network overlap with addresses in another network (whether the network is private or public). In traditional NAT, only one of the addresses is translated.

To configure Twice NAT, you must specify both a destination address and a source address for the match direction, pool or prefix, and translation type.

You can configure application-level gateways (ALGs) for ICMP and traceroute under stateful firewall, NAT, or class-of-service (CoS) rules when Twice NAT is configured in the same service set. These ALGs cannot be applied to flows created by the Packet Gateway Control Protocol (PGCP). Twice NAT does not support other ALGs. By default, the Twice NAT feature can affect IP, TCP, and UDP headers embedded in the payload of ICMP error messages.

Twice NAT, specified in RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*, is fully supported by the Junos OS.

### IPv6 NAT

IPv6-to-IPv6 NAT (NAT66), defined in Internet draft draft-mrw-behave-nat66-01, *IPv6-to-IPv6 Network Address Translation (NAT66)*, is fully supported by the Junos OS.

### Application-level gateway (ALG) Support

The Junos OS supports a number of ALGs. You can use NAT rules to filter incoming traffic based on ALGs. For more information, see [“Network Address Translation Rules Overview” on page 204](#)

### NAT-PT with DNS ALG

NAT-PT and Domain Name System (DNS) ALG are used to facilitate communication between IPv6 hosts and IPv4 hosts. Using a pool of IPv4 addresses, NAT-PT assigns addresses from that pool to IPv6 nodes on a dynamic basis as sessions are initiated across IPv4 or IPv6 boundaries. Inbound and outbound sessions must traverse the same NAT-PT router so that it can track those sessions. RFC 2766, *Network Address Translation - Protocol Translation (NAT-PT)*, recommends the use of NAT-PT for translation between IPv6-only nodes and IPv4-only nodes, and *not* for IPv6-to-IPv6 translation between IPv6 nodes or IPv4-to-IPv4 translation between IPv4 nodes.

DNS is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. The DNS ALG is an application-specific agent that allows an IPv6 node to communicate with an IPv4 node and vice versa.

When DNS ALG is employed with NAT-PT, the DNS ALG translates IPv6 addresses in DNS queries and responses to the corresponding IPv4 addresses and vice versa. IPv4 name-to-address mappings are held in the DNS with “A” queries. IPv6 name-to-address mappings are held in the DNS with “AAAA” queries.

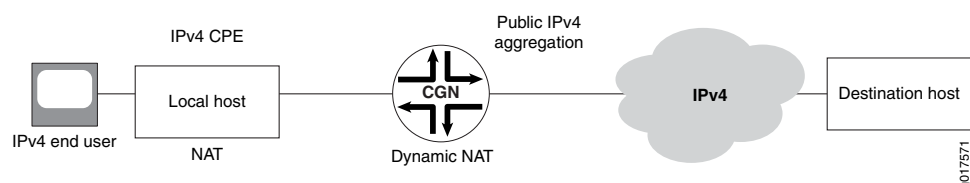


**NOTE:** For IPv6 DNS queries, use the `do-not-translate-AAAA-query-to-A-query` statement at the `[edit applications application application-name]` hierarchy level.

### Dynamic NAT

Dynamic NAT flow is shown in [Figure 4 on page 57](#).

**Figure 4: Dynamic NAT Flow**



With dynamic NAT, you can map a private IP address (source) to a public IP address drawing from a pool of registered (public) IP addresses. NAT addresses from the pool are assigned dynamically. Assigning addresses dynamically also allows a few public IP

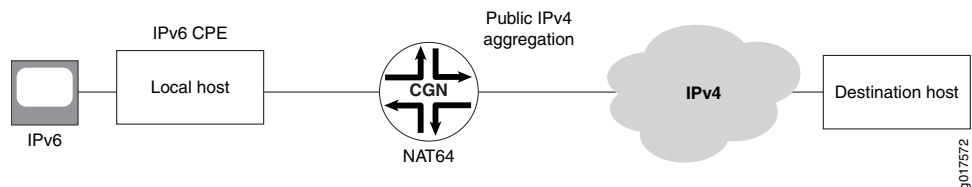
addresses to be used by several private hosts, in contrast with an equal-sized pool required by source static NAT.

For more information about dynamic address translation, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

### Stateful NAT64

Stateful NAT64 flow is shown in [Figure 5 on page 58](#).

**Figure 5: Stateful NAT64 Flow**



Stateful NAT64 is a mechanism to move to an IPv6 network and at the same time deal with IPv4 address depletion. By allowing IPv6-only clients to contact IPv4 servers using unicast UDP, TCP, or ICMP, several IPv6-only clients can share the same public IPv4 server address. To allow sharing of the IPv4 server address, NAT64 translates incoming IPv6 packets into IPv4 (and vice versa).

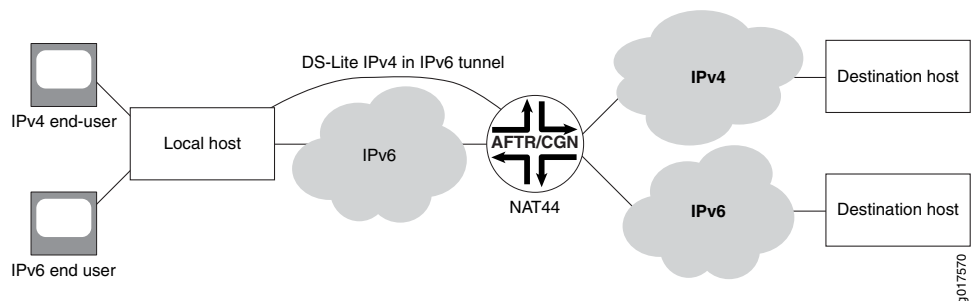
When stateful NAT64 is used in conjunction with DNS64, no changes are usually required in the IPv6 client or the IPv4 server. DNS64 is out of scope of this document because it is normally implemented as an enhancement to currently deployed DNS servers.

Stateful NAT64, specified in RFC 6146, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*, is fully supported by the Junos OS.

### Dual-Stack Lite

Dual-stack lite (DS-Lite) flow is shown in [Figure 6 on page 58](#).

**Figure 6: DS-Lite Flow**



DS-Lite employs IPv4-over-IPv6 tunnels to cross an IPv6 access network to reach a carrier-grade IPv4-IPv4 NAT. This facilitates the phased introduction of IPv6 on the Internet by providing backward compatibility with IPv4.

## Inline Network Address Translation Overview for MPC Types 1, 2, and 3

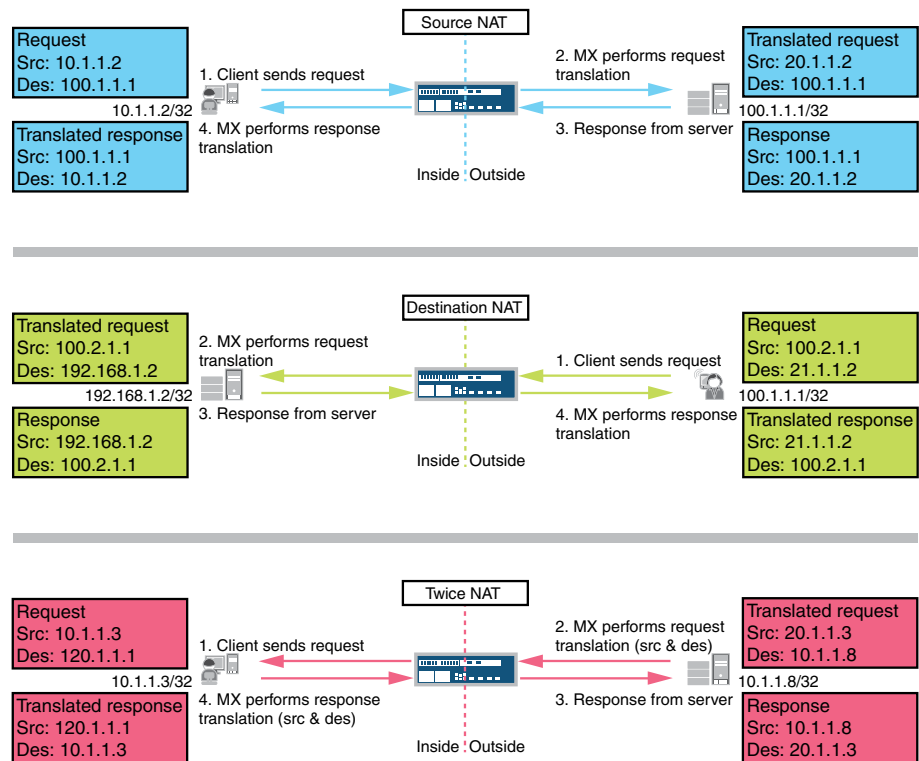
Inline network address translation (NAT) uses the capabilities of the Modular Port Concentrator (MPC) line card, eliminating the need for a MultiServices Dense Port Concentrator (MS-DPC) for NAT. Consequently, you can achieve line-rate, low-latency address translations (up to 120 Gbps per slot). The current implementation provides:

- 1:1 static address mapping
- Bidirectional mapping - source NAT for outbound traffic and destination NAT for inbound traffic
- No limit on number of flows
- Support for Source, destination, and twice NAT, as shown in [Figure 7 on page 59](#)



**NOTE:** Inline NAT generally only the `basic-nat44` translation type, and implements destination NAT and twice NAT by applying NAT at the egress interface or to back-to-back, as shown in the following figure.

Figure 7: Supported Inline NAT Types



g041381

To configure inline NAT, you define your service interface as type `si-` (service-inline) interface. You must also reserve adequate bandwidth for the inline interface. This enables

you to configure both interface or next-hop service-sets used for NAT. The **si-** interface serves as a “virtual service PIC”.



**NOTE:** Only static source NAT is supported. Port translation and dynamic NAT are not supported. An MS-DPC or MS-PIC will still be needed for any stateful-firewall processing.

## Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card

Table 4 on page 60 summarizes feature differences among the Junos OS carrier-grade NAT implementations.

**Table 4: Carrier-Grade NAT—Feature Comparison by Platform**

Feature	MS-DPC	MS-MPC MS-MIC	MPC Types 1, 2, 3 <i>Inline NAT</i>
	MS-100		
	MS-400		
	MS-500		
Static Source NAT	yes	yes	yes
Dynamic Source NAT - Address Only	yes	yes	no
Dynamic Source NAT - NAPT Port Translation with Secured Port Block Allocation	yes	no	no
Dynamic Source NAT - NAPT Port Translation with Deterministic Port Port Block Allocation	yes	no	no
Static Destination NAT	yes	yes	yes
			<p><b>NOTE:</b> Destination NAT can be implemented indirectly. See “<a href="#">Inline Network Address Translation Overview for MPC Types 1, 2, and 3</a>” on page 59</p>
Twice NAT	yes	no	yes
			<p><b>NOTE:</b> Twice NAT can be implemented indirectly. See “<a href="#">Inline Network Address Translation Overview for MPC Types 1, 2, and 3</a>” on page 59</p>
NAPT - Preserve Parity and Port	yes	no	no

Table 4: Carrier-Grade NAT—Feature Comparison by Platform (*continued*)

Feature	MS-DPC MS-100 MS-400 MS-500	MS-MPC MS-MIC	MPC Types 1, 2, 3 <i>Inline NAT</i>
NAPT - EIM/EIF/APP	yes	yes	no
NAT64	yes	yes	no
NAT64 with APP/EIM/EIF	no	yes	no
NAT64 with ALGs <ul style="list-style-type: none"> <li>• FTP</li> <li>• TFTP</li> <li>• SIP</li> <li>• RTSP</li> <li>• PPPT</li> </ul>	no	yes	no
DS-Lite	yes	no	no
6rd	yes	no	no
Overload Pool/Overlap Address Across NAT Pool	yes	no	no
Port Control Protocol	yes	no	no
CGN-PIC	yes	no	no
AMS Support	no	yes	no

[Table 5 on page 61](#) summarizes availability of translation types by type of line card.

Table 5: Carrier-Grade NAT Translation Types

Translation Type	MS-DPC MS-100 MS-400 MS-500	MS-MPC MS-MIC	MPC Types 1, 2, 3 <i>Inline NAT</i>
<b>basic-nat44</b>	yes	yes	yes
<b>basic-nat66</b>	yes	no	no
<b>basic-nat-pt</b>	yes	no	no

Table 5: Carrier-Grade NAT Translation Types (*continued*)

Translation Type	MS-DPC	MS-MPC MS-MIC	MPC Types 1, 2, 3 <i>Inline NAT</i>
	MS-100		
	MS-400		
	MS-500		
<b>deterministic-napt44</b>	yes	no	no
<b>dnat-44</b>	yes	yes	no
<b>dynamic-nat44</b>	yes	yes	no
<b>napt-44</b>	yes	yes	no
<b>napt-66</b>	yes	no	no
<b>napt-pt</b>	yes	no	no
<b>stateful-nat64</b>	yes	yes	no
<b>twice-basic-nat-44</b>	yes	no	no
<b>twice-dynamic-nat-44</b>	yes	no	no
<b>twice-dynamic-napt-44</b>	yes	no	no

### ALGs Available by Default for Junos OS Address Aware NAT

The following application-level gateways (ALGs) listed in [Table 6 on page 63](#) are supported for NAT processing on the listed platforms.

To view the implementation details (port, protocol, and so on) for these Junos OS default applications, locate the Junos OS Default ALG Name in the table and then look up the listed name in the **groups**. For example, for details about TFTP, look up **junos-tftp** as shown.



**TIP:** The Junos OS provides the **junos-alg**, which enables other ALGs to function by handling ALG registrations, causing slow path packets to flow through registered ALGs, and transferring ALG events to the ALG plug-ins. The **junos-alg** ALG is automatically available on the MS-MPC and MS-MIC platforms and does not require further configuration.

```
user@host# show groups junos-defaults applications application junos-tftp
application-protocol tftp;
protocol udp;
destination-port 69;
```

Table 6: ALGs Available by Default

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
Basic TCP ALG	yes	yes	<b>NOTE:</b> Specific Junos ALGs are not supported. However, a feature called TCP tracker, available by default, performs segment ordering and retransmit and connection tracking, validations for TCP connections.
Basic UDP ALG	yes	yes	<b>NOTE:</b> TCP tracker performs limited integrity and validation checks for UDP.
BOOTP	yes	no	<ul style="list-style-type: none"> <li>• <code>junos-bootpc</code></li> <li>• <code>junos-bootps</code></li> </ul>
DCE RPC Services	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-dce-rpc-portmap</code></li> <li>• <code>junos-dcerpc-endpoint-mapper-service</code></li> <li>• <code>junos-dcerpc-msexchange-directory-nsp</code></li> <li>• <code>junos-dcerpc-msexchange-directory-rfr</code></li> <li>• <code>junos-dcerpc-msexchange-information-store</code></li> </ul>
DNS	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-dns-tcp</code></li> <li>• <code>junos-dns-udp</code></li> </ul>
FTP	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-ftp</code></li> </ul>
H323	yes	no	<ul style="list-style-type: none"> <li>• <code>junos-h323</code></li> </ul>
ICMP	yes	yes  <b>NOTE:</b> ICMP messages are handled by default, but PING ALG support is not provided.	<ul style="list-style-type: none"> <li>• <code>junos-icmp-all</code></li> <li>• <code>junos-icmp-ping</code></li> </ul>
IIOp	yes	no	<ul style="list-style-type: none"> <li>• <code>junos-iiop-java</code></li> <li>• <code>junos-iiop-orbix</code></li> </ul>
IP	yes	The TCP tracker, available by default on these platforms, performs limited integrity and validation checks.	<ul style="list-style-type: none"> <li>• <code>junos-ip</code></li> </ul>
NETBIOS	yes	no	<ul style="list-style-type: none"> <li>• <code>junos-netbios-datagram</code></li> <li>• <code>junos-netbios-name-tcp</code></li> <li>• <code>junos-netbios-name-udp</code></li> <li>• <code>junos-netbios-session</code></li> </ul>
NETSHOW	yes	no	<ul style="list-style-type: none"> <li>• <code>junos-netshow</code></li> </ul>
PPTP	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-pptp</code></li> </ul>

Table 6: ALGs Available by Default (*continued*)

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
REALAUDIO	yes	no	<ul style="list-style-type: none"> <li>• <code>junos-realaudio</code></li> </ul>
Sun RPC and RPC Port Map Services	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-rpc-portmap-tcp</code></li> <li>• <code>junos-rpc-portmap-udp</code></li> </ul>
RTSP	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-rtsp</code></li> </ul>
SIP	yes	Yes	<ul style="list-style-type: none"> <li>• <code>junos-sip</code></li> </ul> <p>The SIP <code>callid</code> is <i>not</i> translated in <code>register</code> messages.</p> <p><b>NOTE:</b> SIP sessions are limited to 12 hours (720 minutes) for NAT processing on the MS-MIC and MS-MPC interface cards. There is no time limit for SIP sessions on the MS-DPC.</p>
SNMP	yes	No	<ul style="list-style-type: none"> <li>• <code>junos-snmp-get</code></li> <li>• <code>junos-snmp-get-next</code></li> <li>• <code>junos-snmp-response junos-snmp-trap</code></li> </ul>
SQLNET	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-sqlnet</code></li> </ul>
TFTP	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-tftp</code></li> </ul>
Traceroute	yes	no	<ul style="list-style-type: none"> <li>• <code>junos-traceroute</code></li> </ul>
Unix Remote Shell Service	yes	Yes	<ul style="list-style-type: none"> <li>• <code>junos-rsh</code></li> </ul>
WINFrame	yes	No	<ul style="list-style-type: none"> <li>• <code>junos-citrix-winframe</code></li> <li>• <code>junos-citrix-winframe-udp</code></li> </ul>
TALK-UDP	No	Yes	<ul style="list-style-type: none"> <li>• <code>junos-talk-udp</code></li> </ul>
MS RPC	No	Yes	<ul style="list-style-type: none"> <li>• <code>junos-rpc-portmap-tcp</code></li> <li>• <code>junos-rpc-portmap-udp</code></li> <li>• <code>junos-rpc-services-tcp</code></li> <li>• <code>junos-rpc-services-udp</code></li> </ul>

## Port Control Protocol Overview

The Port Control Protocol (PCP) provides a mechanism to control the forwarding of incoming packets by upstream devices such as NAT44, and firewall devices, and a mechanism to reduce application keep-alive traffic. PCP is designed to be implemented in the context of both Carrier-Grade NATs (CGNs) and small NATs (for example, residential NATs). PCP allows hosts to operate servers for a long time (as in the case of a webcam) or a short time (for example, while playing a game or on a phone call) when

behind a NAT device, including when behind a CGN operated by their Internet service provider. PCP allows applications to create mappings from an external IP address and port to an internal IP address and port. These mappings are required for successful inbound communications destined to machines located behind a NAT or a firewall. After creating a mapping for incoming connections, it is necessary to inform remote computers about the IP address and port for the incoming connection. This is usually done in an application-specific manner.

PCP consists of the following components:

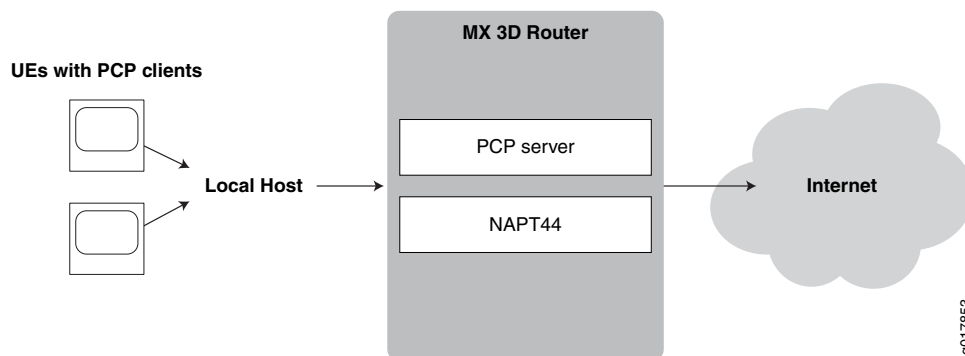
- PCP client—A host or gateway that issues PCP requests to a PCP server in order to obtain and control resources.
- PCP server—Typically a CGN gateway or co-located server that receives and processes PCP requests

Many NAT-friendly applications send frequent application-level messages to ensure their session are not be timed out by a NAT. These applications can reduce the frequency of such NAT keep-alive messages by using PCP to learn and influence the NAT mapping lifetime. This helps reduce bandwidth on the subscriber's access network, traffic to the server, and battery consumption on mobile devices.

The Junos OS enables configuring PCP servers for mapping flows using NAPT44 capabilities such as port forwarding and port block allocation. Flows can be processed from these sources:

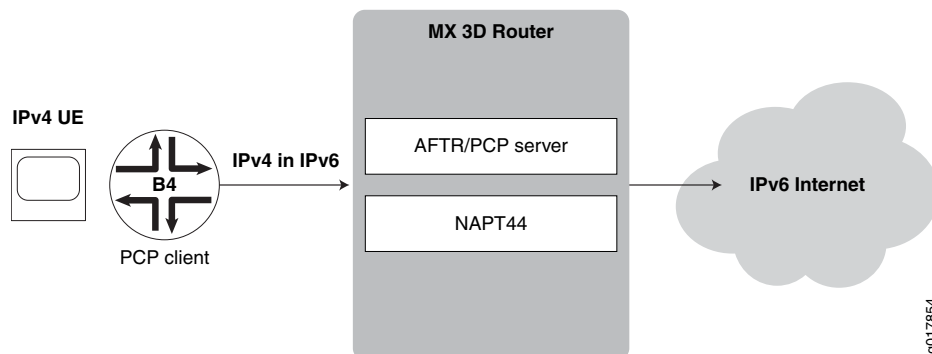
- Traffic containing PCP requests received directly from UEs as shown in [Figure 8 on page 65](#).

**Figure 8: Basic PCP NAPT44 Topology**



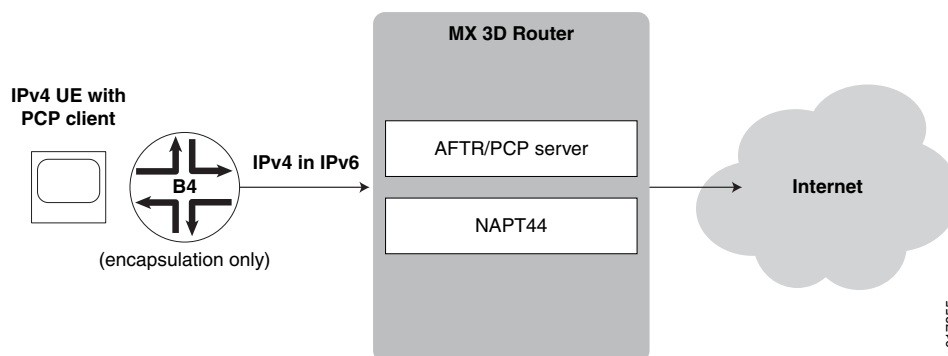
- Mapping of traffic containing PCP requests added by a router functioning as a DS-Lite software initiator (B4). This mode, known as *DS-Lite plain mode*, is show in [Figure 9 on page 66](#)

Figure 9: PCP with DS-Lite Plain Mode



- Mapping of traffic containing PCP requests initiated by directly by UEs and encapsulated by a router functioning as a DS-Lite software initiator (B4). This mode, known as *DS-Lite tunnel mode*, is shown in [Figure 10 on page 66](#).

Figure 10: PCP with DS-Lite Tunnel Mode



**NOTE:** The Junos OS does not support deterministic port block allocation for PCP-originated traffic.

**Related Documentation**

- [Configuring Port Control Protocol on page 257](#)

## Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card

[Table 4 on page 60](#) summarizes feature differences among the Junos OS carrier-grade NAT implementations.

Table 7: Carrier-Grade NAT—Feature Comparison by Platform

Feature	MS-DPC		
	MS-100		
	MS-400	MS-MPC	MPC Types 1, 2, 3
	MS-500	MS-MIC	<i>Inline NAT</i>
Static Source NAT	yes	yes	yes
Dynamic Source NAT - Address Only	yes	yes	no
Dynamic Source NAT - NAT Port Translation with Secured Port Block Allocation	yes	no	no
Dynamic Source NAT - NAT Port Translation with Deterministic Port Block Allocation	yes	no	no
Static Destination NAT	yes	yes	yes
			NOTE: Destination NAT can be implemented indirectly. See <a href="#">“Inline Network Address Translation Overview for MPC Types 1, 2, and 3”</a> on page 59
Twice NAT	yes	no	yes
			NOTE: Twice NAT can be implemented indirectly. See <a href="#">“Inline Network Address Translation Overview for MPC Types 1, 2, and 3”</a> on page 59
NAPT - Preserve Parity and Port	yes	no	no
NAPT - EIM/EIF/APP	yes	yes	no
NAT64	yes	yes	no
NAT64 with APP/EIM/EIF	no	yes	no
NAT64 with ALGs	no	yes	no
<ul style="list-style-type: none"> <li>• FTP</li> <li>• TFTP</li> <li>• SIP</li> <li>• RTSP</li> <li>• PPPT</li> </ul>			

Table 7: Carrier-Grade NAT—Feature Comparison by Platform (*continued*)

Feature	MS-DPC	MS-MPC MS-MIC	MPC Types 1, 2, 3 <i>Inline NAT</i>
	MS-100		
	MS-400		
	MS-500		
DS-Lite	yes	no	no
6rd	yes	no	no
Overload Pool/Overlap Address Across NAT Pool	yes	no	no
Port Control Protocol	yes	no	no
CGN-PIC	yes	no	no
AMS Support	no	yes	no

[Table 5 on page 61](#) summarizes availability of translation types by type of line card.

Table 8: Carrier-Grade NAT Translation Types

Translation Type	MS-DPC	MS-MPC MS-MIC	MPC Types 1, 2, 3 <i>Inline NAT</i>
	MS-100		
	MS-400		
	MS-500		
<b>basic-nat44</b>	yes	yes	yes
<b>basic-nat66</b>	yes	no	no
<b>basic-nat-pt</b>	yes	no	no
<b>deterministic-napt44</b>	yes	no	no
<b>dnat-44</b>	yes	yes	no
<b>dynamic-nat44</b>	yes	yes	no
<b>napt-44</b>	yes	yes	no
<b>napt-66</b>	yes	no	no
<b>napt-pt</b>	yes	no	no

Table 8: Carrier-Grade NAT Translation Types (*continued*)

Translation Type	MS-DPC		
	MS-100		
	MS-400	MS-MPC	MPC Types 1, 2, 3
	MS-500	MS-MIC	<i>Inline NAT</i>
stateful-nat64	yes	yes	no
twice-basic-nat-44	yes	no	no
twice-dynamic-nat-44	yes	no	no
twice-dynamic-napt-44	yes	no	no

**Related Documentation** • [Junos OS CGNAT Implementation Overview on page 53](#)

## ALGs Available by Default for Junos OS Address Aware NAT

The following application-level gateways (ALGs) listed in [Table 6 on page 63](#) are supported for NAT processing on the listed platforms.

To view the implementation details (port, protocol, and so on) for these Junos OS default applications, locate the Junos OS Default ALG Name in the table and then look up the listed name in the **groups**. For example, for details about TFTP, look up **junos-tftp** as shown.



**TIP:** The Junos OS provides the **junos-alg**, which enables other ALGs to function by handling ALG registrations, causing slow path packets to flow through registered ALGs, and transferring ALG events to the ALG plug-ins. The **junos-alg** ALG is automatically available on the MS-MPC and MS-MIC platforms and does not require further configuration.

```
user@host# show groups junos-defaults applications application junos-tftp
application-protocol tftp;
protocol udp;
destination-port 69;
```

Table 9: ALGs Available by Default

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
Basic TCP ALG	yes	yes	<b>NOTE:</b> Specific Junos ALGs are not supported. However, a feature called TCP tracker, available by default, performs segment ordering and retransmit and connection tracking, validations for TCP connections.

Table 9: ALGs Available by Default (*continued*)

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
Basic UDP ALG	yes	yes	<b>NOTE:</b> TCP tracker performs limited integrity and validation checks for UDP.
BOOTP	yes	no	<ul style="list-style-type: none"> <li>• junos-bootpc</li> <li>• junos-bootps</li> </ul>
DCE RPC Services	yes	yes	<ul style="list-style-type: none"> <li>• junos-dce-rpc-portmap</li> <li>• junos-dcerpc-endpoint-mapper-service</li> <li>• junos-dcerpc-msexchange-directory-nsp</li> <li>• junos-dcerpc-msexchange-directory-rfr</li> <li>• junos-dcerpc-msexchange-information-store</li> </ul>
DNS	yes	yes	<ul style="list-style-type: none"> <li>• junos-dns-tcp</li> <li>• junos-dns-udp</li> </ul>
FTP	yes	yes	<ul style="list-style-type: none"> <li>• junos-ftp</li> </ul>
H323	yes	no	<ul style="list-style-type: none"> <li>• junos-h323</li> </ul>
ICMP	yes	yes  <b>NOTE:</b> ICMP messages are handled by default, but PING ALG support is not provided.	<ul style="list-style-type: none"> <li>• junos-icmp-all</li> <li>• junos-icmp-ping</li> </ul>
IIOp	yes	no	<ul style="list-style-type: none"> <li>• junos-iiop-java</li> <li>• junos-iiop-orbix</li> </ul>
IP	yes	The TCP tracker, available by default on these platforms, performs limited integrity and validation checks.	<ul style="list-style-type: none"> <li>• junos-ip</li> </ul>
NETBIOS	yes	no	<ul style="list-style-type: none"> <li>• junos-netbios-datagram</li> <li>• junos-netbios-name-tcp</li> <li>• junos-netbios-name-udp</li> <li>• junos-netbios-session</li> </ul>
NETSHOW	yes	no	<ul style="list-style-type: none"> <li>• junos-netshow</li> </ul>
PPTP	yes	yes	<ul style="list-style-type: none"> <li>• junos-pptp</li> </ul>
REALAUDIO	yes	no	<ul style="list-style-type: none"> <li>• junos-realaudio</li> </ul>
Sun RPC and RPC Port Map Services	yes	yes	<ul style="list-style-type: none"> <li>• junos-rpc-portmap-tcp</li> <li>• junos-rpc-portmap-udp</li> </ul>

Table 9: ALGs Available by Default (*continued*)

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
RTSP	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-rtsp</code></li> </ul>
SIP	yes	Yes	<ul style="list-style-type: none"> <li>• <code>junos-sip</code></li> </ul> <p>The SIP <code>callid</code> is <i>not</i> translated in <code>register</code> messages.</p> <p><b>NOTE:</b> SIP sessions are limited to 12 hours (720 minutes) for NAT processing on the MS-MIC and MS-MPC interface cards. There is no time limit for SIP sessions on the MS-DPC.</p>
SNMP	yes	No	<ul style="list-style-type: none"> <li>• <code>junos-snmp-get</code></li> <li>• <code>junos-snmp-get-next</code></li> <li>• <code>junos-snmp-response junos-snmp-trap</code></li> </ul>
SQLNET	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-sqlnet</code></li> </ul>
TFTP	yes	yes	<ul style="list-style-type: none"> <li>• <code>junos-tftp</code></li> </ul>
Traceroute	yes	no	<ul style="list-style-type: none"> <li>• <code>junos-traceroute</code></li> </ul>
Unix Remote Shell Service	yes	Yes	<ul style="list-style-type: none"> <li>• <code>junos-rsh</code></li> </ul>
WINFrame	yes	No	<ul style="list-style-type: none"> <li>• <code>junos-citrix-winframe</code></li> <li>• <code>junos-citrix-winframe-udp</code></li> </ul>
TALK-UDP	No	Yes	<ul style="list-style-type: none"> <li>• <code>junos-talk-udp</code></li> </ul>
MS RPC	No	Yes	<ul style="list-style-type: none"> <li>• <code>junos-rpc-portmap-tcp</code></li> <li>• <code>junos-rpc-portmap-udp</code></li> <li>• <code>junos-rpc-services-tcp</code></li> <li>• <code>junos-rpc-services-udp</code></li> </ul>

**Related Documentation** • [ALG Descriptions on page 126](#)

## Tunneling Services for IPv4-to-IPv6 Transition Overview

The Junos OS enables service providers to transition to IPv6 by using software encapsulation and decapsulation techniques. A software is a tunnel that is created between software Customer Premises Equipment (CPE). A software CPE can share a unique common internal state for multiple softwares, making it a very light and scalable solution. When you use softwares, you need not maintain an interface infrastructure for each software, unlike a typical mesh of generic routing encapsulation (GRE) tunnels that would require you to do so. A software initiator at the customer end encapsulates native packets and tunnels them to a software concentrator at the service provider. The software

concentrator decapsulates the packets and sends them to their destination. A softwire is created when a softwire concentrator receives the first tunneled packet of a flow and prepares for flow processing. The softwire exists as long as the softwire concentrator is providing flows for routing. A flow counter is maintained; when the number of active flows is 0, the softwire is deleted. Statistics are kept for both flows and softwires.

Softwire addresses are not specifically configured under any physical or virtual interface. Therefore, the number of established softwires does not affect throughput, and scalability is independent of the number of interfaces. The scalability is only limited to the number of flows that the platform (services DPC or PIC) can support.

This topic contains the following sections:

- [6to4 Overview on page 72](#)
- [DS-Lite Softwires—IPv4 over IPv6 on page 74](#)
- [6rd Softwires—IPv6 over IPv4 on page 74](#)

## 6to4 Overview

- [Basic 6to4 on page 72](#)
- [6to4 Anycast on page 73](#)
- [6to4 Provider-Managed Tunnels on page 73](#)

---

### Basic 6to4

6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network (generally the IPv4 Internet) without the need to configure explicit tunnels. 6to4 is described in RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds*. 6to4 is especially relevant during the initial phases of deployment to full, native IPv6 connectivity, since IPv6 is not required on nodes between the host and the destination. However, it is intended only as a transition mechanism and is not meant to be used permanently.

6to4 can be used by an individual host, or by a local IPv6 network. When used by a host, it must have a global IPv4 address connected, and the host is responsible for the encapsulation of outgoing IPv6 packets and the decapsulation of incoming 6to4 packets. If the host is configured to forward packets for other clients, often a local network, it is then a router.

There are two kinds of 6to4 virtual routers: border routers and relay routers. A 6to4 border router is an IPv6 router supporting a 6to4 pseudointerface, and is normally the border router between an IPv6 site and a wide-area IPv4 network. A relay router is a 6to4 router configured to support transit routing between 6to4 addresses and pure native IPv6 addresses.

In order for a 6to4 host to communicate with the native IPv6 Internet, its IPv6 default gateway must be set to a 6to4 address which contains the IPv4 address of a 6to4 relay router. To avoid the need for users to set this up manually, the Anycast address of 192.88.99.1 has been allocated to send packets to a 6to4 relay router. Note that when wrapped in 6to4 with the subnet and hosts fields set to zero, this IPv4 address (192.88.99.1) becomes the IPv6 address 2002:c058:6301::. To ensure BGP routing

propagation, a short prefix of 192.88.99.0/24 has been allocated for routes pointed at 6to4 relay routers that use this Anycast IP address. Providers willing to provide 6to4 service to their clients or peers should advertise the Anycast prefix like any other IP prefix, and route the prefix to their 6to4 relay.

Packets from the IPv6 Internet to 6to4 systems must be sent to a 6to4 relay router by normal IPv6 routing methods. The specification states that such relay routers must only advertise 2002::/16 and not subdivisions of it to prevent IPv4 routes from polluting the routing tables of IPv6 routers. From there they can then be sent over the IPv4 Internet to the destination.

### 6to4 Anycast

Router 6to4 assumes that 6to4 routers and relays are managed and configured cooperatively. In particular, 6to4 sites must configure a relay router to carry the outbound traffic, which becomes the default IPv6 router (except for 2002::/16). The objective of the Anycast variant, defined in RFC 3068, *An Anycast Prefix for 6to4 Relay Routers*, is to avoid the need for such configuration. This makes the solution available for small or domestic users, even those with a single host or simple home gateway instead of a border router. This is achieved by defining 192.88.99.1 as the default IPv4 address for a 6to4 relay, and 2002:c058:6301:: as the default IPv6 router prefix (“well-known prefix”) for a 6to4 site.

RFC 6343, *Advisory Guidelines for 6to4 Deployment*, published in August 2011, identifies a wide range of problems associated with the use of unmanaged 6to4 Anycast relay routers.

### 6to4 Provider-Managed Tunnels

A solution to many problems associated with unmanaged Anycast 6to4 is presented in IETF informational draft draft-kuarsingh-v6ops-6to4-provider-managed-tunnel-02, *6to4 Provider-Managed Tunnels (PMT)*. That document, a “work in progress,” proposes a solution that allows providers to exercise greater control over the routing of 6to4 traffic.

Anycast 6to4 implies a default configuration for the user site. It does not require any particular user action. It does require an IPv4 Anycast route to be in place to a relay at 192.88.99.1. Traffic does not necessarily return to the same 6to4 gateway because of the the “well-known” 6to4 prefix used and advertised by all 6to4 traffic.

6to4 provider-managed tunnels (PMTs) facilitate the management of 6to4 tunnels using an Anycast configuration. 6to4 PMT enables service providers to improve 6to4 operation when network conditions provide suboptimal performance or break normal 6to4 operation. 6to4 PMT provides a stable provider prefix and forwarding environment by utilizing existing 6to4 relays with an added function of IPv6 prefix translation that controls the flow of return traffic.

The 6to4 managed tunnel model behaves like a standard 6to4 service between the customer IPv6 host or gateway and the 6to4 PMT relay (within the provider domain). The 6to4-PMT relay shares properties with 6rd (RFC5969) by decapsulating and forwarding embedded IPv6 flows, within an IPv4 packet, to the IPv6 Internet. The model provides an additional function which translates the source 6to4 prefix to a provider assigned prefix which is not found in 6rd (RFC5969) or traditional 6to4 operation. The

6to4-PMT relay provides a stateless (or stateful) mapping of the 6to4 prefix to a provider-supplied prefix by mapping the embedded IPv4 address in the 6to4 prefix to the provider prefix.

## DS-Lite Softwires—IPv4 over IPv6

When an Internet service provider (ISP) begins to allocate new subscriber home IPv6 addresses and IPv6-capable equipment, dual-stack lite (DS-Lite) provides a method for the private IPv4 addresses behind the IPv6 customer edge (CE) WAN equipment to reach the IPv4 network. DS-Lite enables IPv4 customers to continue to access the Internet using their current hardware by using a softwire initiator, referred to as a Basic Bridging Broadband (B4), at the customer edge to encapsulate IPv4 packets into IPv6 packets and tunnel them over an IPv6 network to a softwire concentrator, referred to as an Address Family Transition Router (AFTR), for decapsulation. DS-Lite creates the IPv6 softwires that terminate on the services PIC. Packets coming out of the softwire can then have other services such as NAT applied on them.

DS-Lite is supported on Multiservices 100, 400, and 500 PICs on M Series routers and on MX Series routers equipped with Multiservices Dense Port Concentrator (DPCs).



**NOTE:** IPv6 Provider Edge (6PE), or MPLS-enabled IPv6, is available for ISPs with MPLS-enabled networks. These networks now can use Multiprotocol BGP (MP-BGP) to provide connectivity between the DS-Lite B4 and AFTR (or any two IPv6 nodes). DS-Lite properly handles encapsulation and decapsulation despite the presence of additional MPLS header information.

For more information on DS-Lite softwires, see the IETF draft *Dual Stack Lite Broadband Deployments Following IPv4 Exhaustion*.



**NOTE:** The most recent IETF draft documentation for DS-Lite uses new terminology:

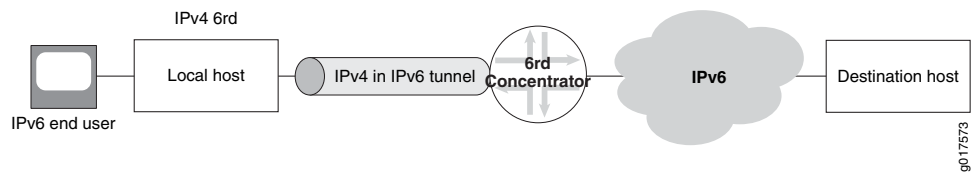
- The term *softwire initiator* has been replaced by *B4*.
- The term *softwire concentrator* has been replaced by *AFTR*.

The Junos OS documentation generally uses the original terms when discussing configuration in order to be consistent with the command-line interface (CLI) statements used to configure DS-Lite.

## 6rd Softwires—IPv6 over IPv4

6rd softwire flow is shown in [Figure 11 on page 75](#).

Figure 11: 6rd Software Flow



The Junos OS supports a 6rd software concentrator on a services DPC or PIC to facilitate rapid deployment of IPv6 service to subscribers on native IPv4 CE WANs. IPv6 packets are encapsulated in IPv4 packets by a software initiator at the CE WAN. These packets are tunneled to a software concentrator residing on a multiservices DPC (branch relay). A software is created when IPv4 packets containing IPv6 destination information are received at the software concentrator, which decapsulates IPv6 packets and forwards them for IPv6 routing. All of these functions are performed in a single pass of the services PIC.

In the reverse path, IPv6 packets are sent to the Services DPC where they are encapsulated in IPv4 packets corresponding to the proper software and sent to the CE WAN.

The software concentrator creates softwires as the IPv4 packets are received from the CE WAN side or IPv6 packets are received from the Internet. A 6rd software on the Services DPC is identified by the 3-tuple containing the service set ID, CE software initiator IPv4 address, and software concentrator IPv4 address. IPv6 flows are also created for the encapsulated IPv6 payload, and are associated with the specific software that carried them in the first place. When the last IPv6 flow associated with a software ends, the software is deleted. This simplifies configuration and there is no need to create or manage tunnel interfaces.

6rd is supported on Multiservices 100, 400, and 500 PICs on M Series and T Series routers, and on MX Series platforms equipped with Multiservices DPCs.

For more information on 6rd softwires, see RFC 5969, *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification*.

#### Related Documentation

- [Network Address Translation Overview for MS-DPC, MS-MPC, and MS-MIC Line Cards on page 54](#)
- [Configuring a 6rd Software Concentrator on page 344](#)
- [Configuring a DS-Lite Software Concentrator on page 343](#)
- [Configuring Software Rules on page 345](#)
- [Configuring Service Sets for Software on page 346](#)

## Understanding Junos VPN Site Secure

Junos VPN Site Secure is a suite of IPsec features supported on multiservices line cards (MS-DPC, MS-MPC, and MS-MIC), and was referred to as IPsec services in Junos releases earlier than 13.2. In Junos OS Release 13.2 and later, the term IPsec features is used exclusively to refer to the IPsec implementation on Adaptive Services and Encryption

Services PICs. This topic provides you an overview of Junos VPN Site Secure, and has the following sections:



NOTE:

For a list of the IPsec and IKE standards supported by the Junos OS, see the *Junos OS Hierarchy and RFC Reference*.

- [IPsec on page 76](#)
- [Security Associations on page 76](#)
- [IKE on page 77](#)
- [Comparison of IPsec on ES PICs and Junos VPN Site Secure on Multiservices Line Cards on page 77](#)

## IPsec

The IPsec architecture provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPsec, the Junos OS also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs).

IPsec also defines a security association and key management framework that can be used with any network-layer protocol. The SA specifies what protection policy to apply to traffic between two IP-layer entities. IPsec provides secure tunnels between two peers.

## Security Associations

To use IPsec security services, you create SAs between hosts. An SA is a simplex connection that enables two hosts to communicate with each other securely by means of IPsec. There are two types of SAs:

- Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. Manual SAs statically define the security parameter index (SPI) values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.
- Dynamic SAs require additional configuration. With dynamic SAs, you configure IKE first and then the SA. IKE creates dynamic security associations; it negotiates SAs for IPsec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway. This connection is then used to dynamically agree upon keys and other data used by the dynamic IPsec SA. The IKE SA is negotiated first and then used to protect the negotiations that determine the dynamic IPsec SAs.

## IKE

IKE is a key management protocol that creates dynamic SAs; it negotiates SAs for IPsec. An IKE configuration defines the algorithms and keys used to establish a secure connection with a peer security gateway.

IKE performs the following tasks:

- Negotiates and manages IKE and IPsec parameters.
- Authenticates secure key exchange.
- Provides mutual peer authentication by means of shared secrets (not passwords) and public keys.
- Provides identity protection (in main mode).

Two versions of the IKE protocol (IKEv1 and IKEv2) are supported now. IKE negotiates security attributes and establishes shared secrets to form the bidirectional IKE SA. In IKE, inbound and outbound IPsec SAs are established and the IKE SA secures the exchanges. Starting with Junos OS Release 11.4, both IKEv1 and IKEv2 are supported by default on all M Series, MX Series, and T Series routers. IKE also generates keying material, provides Perfect Forward Secrecy, and exchanges identities.

## Comparison of IPsec on ES PICs and Junos VPN Site Secure on Multiservices Line Cards

Table 10 on page 77 compares the top-level configuration of IPsec features on the ES PIC interfaces, and IPsec on the Adaptive Services PICs and Junos VPN Site Secure on Multiservices Line Cards.

**Table 10: Statement Equivalents for ES and AS Interfaces**

ES PIC Configuration	AS and MultiServices Line Cards Configuration
[edit security ipsec] proposal {...}	[edit services ipsec-vpn ipsec] proposal {...}
[edit security ipsec] policy {...}	[edit services ipsec-vpn ipsec] policy {...}
[edit security ipsec] security-association sa-dynamic {...}	[edit services ipsec-vpn rule <i>rule-name</i> ] term <i>term-name</i> match-conditions {...} then dynamic {...}]
[edit security ipsec] security-association sa-manual {...}	[edit services ipsec-vpn rule <i>rule-name</i> ] term <i>term-name</i> match-conditions {...} then manual {...}]
[edit security ike] proposal {...}	[edit services ipsec-vpn ike] proposal {...}
[edit security ike] policy {...}	[edit services ipsec-vpn ike] policy {...}
Not available	[edit services ipsec-vpn] rule-set {...}

Table 10: Statement Equivalents for ES and AS Interfaces (*continued*)

ES PIC Configuration	AS and MultiServices Line Cards Configuration
Not available	[edit services ipsec-vpn] service-set {...}
[edit interfaces es- <i>fpc/pic/port</i> ] tunnel source <i>address</i>	[edit services ipsec-vpn service-set <i>set-name</i> ] ipsec-vpn local-gateway <i>address</i> ]
[edit interfaces es- <i>fpc/pic/port</i> ] tunnel destination <i>address</i>	[edit services ipsec-vpn rule <i>rule-name</i> ] remote-gateway <i>address</i>



**NOTE:** Although many of the same statements and properties are valid on both platforms (MultiServices and ES), the configurations are not interchangeable. You must commit a complete configuration for the PIC type that is installed in your router.

#### Related Documentation

- [Authentication Algorithms](#)
- [Encryption Algorithms](#)
- [IPsec Protocols](#)
- [Service Sets](#)
- [Configuring Security Associations](#)
- [IPsec Hierarchy Level](#)

## Layer 2 Tunneling Protocol Overview

L2TP is defined in RFC 2661, *Layer Two Tunneling Protocol (L2TP)*.

L2TP facilitates the tunneling of PPP packets across an intervening network in a way that is as transparent as possible to both end users and applications. It employs access profiles for group and individual user access, and uses authentication to establish secure connections between the two ends of each tunnel. Multilink PPP functionality is also supported.

The L2TP services are supported on the following routers only:

- M7i routers with AS PICs
- M10i routers with AS and MultiServices 100 PICs
- M120 routers with AS, MultiServices 100, and MultiServices 400 PICs

For more information, see “[L2TP Services Configuration Overview](#)” on page 579.

#### Related Documentation

- [L2TP Services Configuration Overview on page 579](#)
- [AS PIC Redundancy for L2TP Services on page 589](#)

- [L2TP Minimum Configuration on page 580](#)
- [Examples: Configuring L2TP Services on page 593](#)

## Voice Services Overview

Adaptive services interfaces include a voice services feature that allows you to specify interface type **lsq-fpc/pic/port** to accommodate voice over IP (VoIP) traffic. This interface uses compressed RTP (CRTP), which is defined in RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*.

CRTP enables VoIP traffic to use low-speed links more effectively, by compressing the 40-byte IP/UDP/RTP header down to 2 to 4 bytes in most cases.

Voice services on the AS and MultiServices PICs support single-link PPP-encapsulated IPv4 traffic over the following physical interface types: ATM2, DS3, E1, E3, OC3, OC12, STM1, and T1, including the channelized versions of these interfaces.

Voice services do not require a separate service rules configuration.

Voice services also support LFI on Juniper Networks M Series Multiservice Edge routers, except the M320 router. For more information about configuring voice services, see [“Configuring Services Interfaces for Voice Services” on page 696](#).

For link services IQ interfaces (**lsq**) only, you can configure CRTP with multiclass MLPPP (MCML). MCML greatly simplifies packet ordering issues that occur when multiple links are used. Without MCML, all voice traffic belonging to a single flow is hashed to a single link in order to avoid packet ordering issues. With MCML, you can assign voice traffic to a high-priority class, and you can use multiple links. For more information about MCML support on link services IQ interfaces, see [“Configuring Link Services and CoS on Services PICs” on page 646](#).

### Related Documentation

- [Configuring Services Interfaces for Voice Services on page 696](#)
- [Configuring Encapsulation for Voice Services on page 699](#)
- [Configuring Network Interfaces for Voice Services on page 700](#)
- [Examples: Configuring Voice Services on page 701](#)

## HTTP URL Tracking and Policy Control for Client Requests

The URL manipulation capability in the service plane allows an administrator to enter all the URLs associated with an action. An administrator can now enter URLs and actions in the service plane and apply them to the traffic associated with an interface and a subscriber by using the existing functions.



**NOTE:** The URL manipulation capability is supported only when the Junos OS Extension-Provider packages are installed and configured on the device.

In Junos OS releases earlier than 12.3, the extension-provider packages were variously referred to as Junos Services Framework (JSF), MP-SDK, and eJunos.

The HTTP URL manipulation allows routers to:

- Monitor HTTP transactions in the service plane and identify matching incoming HTTP requests with preconfigured URLs. When a matching HTTP request is found, the associated action and preconfigured URL are applied to the transaction.
- Maintain the statistics of HTTP requests that match the preconfigured URLs. Such statistics must be maintained per policy on a per-rule or per-term basis across all service sets.
- Display the current statistics for all visible HTTP-URL matches.
- Scale 50,000 HTTP transactions per second on a single MS-DPC network processing unit.

### Guidelines for Configuring HTTP URL Monitoring for Client Requests

HTTP URL manipulation can be configured with service rules containing a sequence of terms. The URL rules are evaluated based on the longest prefix or suffix matches. The rules and terms are configured if:

- Multiple hostnames are specified in a match condition with an OR operator (that is, “any” is a potential match).
- Multiple request-URLs are specified in a match condition with an OR operator (that is, “any” is a potential match).
- The “discard” action causes HTTP requests matched to URLs to be dropped (stateful).
- The “accept” action causes HTTP requests matched to URLs to be allowed (stateful).
- The “log-request” action causes HTTP requests matched to URLs to be logged (fast log, once per transaction).
- The “count” action causes HTTP requests matched to URLs to be counted against the specified rule or term. The total number is the total of all service sets in which the rule or terms exists.
- The “discard” action can be combined only with the “log-request” action.
- The “accept” action can be combined with the “log-request” and “count” actions.
- If any given HTTP request matches more than one rule or term, the action applied is undeterministic and may be any of the matched rules or terms.
- The number of rules, terms, url-lists, and individual clauses in the rules, terms, and url-lists are limited by service-plane memory. No hard limits are imposed.

- If a hostname is not specified, then "\*" (any) is assumed. Similarly, if a request-URL is not specified, then "\*" (any) is assumed. Matching of hostnames and request-URLs to the HTTP request follows the same process described for url-lists. However, a match happens only when both the hostname and the request-URL match an entry in the same term of a rule.
- Multiple "url" and "url-list" clauses may be entered for the same "from {}" clause.

## Configuring HTTP URL Tracking and Policy Control

To configure an HTTP URL Tracking and Policy Control, include the **url-rule url-rule-name** statement at the **[edit services hcm]** hierarchy level:

```
services {
  hcm {
    url-rule url-rule-name {
      term term-num {
        from {
          url-list url-list-name;
          url url_identifier {
            host hostname;
            request-url page-name;
          }
        }
        then {
          discard;
          accept;
          count;
          log-request;
        }
      }
    }
    url-rule-set url-rule-set-name {
      url-rule rule1;
      url-rule rule2;
    }
  }
}
```

Each HCM rule consists of a set of terms, similar to a firewall filter. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software.

### Related Documentation

- [HTTP Content Manager \(HCM\)](#)
- [HTTP URL Tracking and Policy Control for Client Requests on page 79](#)
- `show services hcm statistics`

## Class of Service Overview

---

The CoS configuration available for the AS PIC enables you to configure Differentiated Services (DiffServ) code point (DSCP) marking and forwarding-class assignment for packets transiting the AS PIC. You can configure the CoS service alongside the stateful firewall and NAT services, using a similar rule structure. The component structures are described in detail in the *Junos OS Class of Service Library for Routing Devices*.

Standards for Differentiated Services are described in the following documents:

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2475, *An Architecture for Differentiated Services*



**NOTE:** CoS BA classification is not supported on services interfaces.

---

### Related Documentation

- [Restrictions and Cautions for CoS Configuration on Services Interfaces on page 716](#)
- [Configuring CoS Rules on page 717](#)
- [Configuring CoS Rule Sets on page 722](#)
- [Examples: Configuring CoS on Services Interfaces on page 722](#)

## Configuring Routing Services on Multiservices MIC and MPC (MS-MIC and MS-MPC)

---

In Junos OS Release 13.2, Juniper Networks introduces the Multiservices Modular Interfaces Card (MS-MIC) and the Multiservices Modular PIC Concentrator (MS-MPC) that provide improved scaling and high performance. The MS-MIC and MS-MPC have enhanced memory (16 GB for MS-MIC, 32 GB per NPU of MS-MPC) and processing capabilities.

The services interfaces on MS-MPC and MS-MIC are identified in the configuration with an **ms-** prefix (for example, **ms-1/2/1**). The following services packages come preinstalled and preconfigured on MS-MICs and MS-MPCs in Junos OS Release 13.2:

- Junos Traffic Vision (formerly referred to as Jflow)
- Junos Address Aware (formerly referred to as NAT features)
- Junos VPN Site Secure (formerly referred to as IPsec features)
- Junos Network Secure (formerly referred to as the Stateful Firewall feature)
- Junos Services Crypto Base PIC Package
- Junos Services Application Level Gateways



**NOTE:** You can check the default packages on an MS-MIC or MS-MPC by executing the `show extension-provider system packages interface ms-interface` operational mode command.

Table 11 on page 83 lists the platforms on which the MS-MIC and MS-MPC are supported.

**Table 11: MX Series Routers that Support MS-MIC and MS-MPC**

	MX5	MX10	MX40	MX80	MX240	MX480	MX960	MX2010	MX2020
<b>MS-MIC</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>NOTE:</b> Only Junos Traffic Vision is supported.									
<b>MS-MPC</b>	No	No	No	No	Yes	Yes	Yes	No	No

You can install an MS-MIC on one of the following line cards:

- MPC-Type1
- MPC-Type2

This document contains the following topics:

- [Key Features Supported on Multiservices MIC and MPC \(MS-MIC and MS-MPC\) on page 83](#)
- [Example: Configuring Flow Monitoring on MS-MIC and MS-MPC on page 86](#)
- [Understanding Aggregated Multiservices Interfaces on page 93](#)
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\) on page 94](#)
- [Example: Configuring Next-Hop Style Services on an Aggregated Multiservices Interface on page 99](#)
- [Example: Configuring Junos VPN Site Secure on MS MIC and MS-MPC on page 102](#)
- [Example: NAPT Configuration for the MS-MPC on page 113](#)

### Key Features Supported on Multiservices MIC and MPC (MS-MIC and MS-MPC)

This section lists the following key Junos OS features supported on the MS-MIC and MS-MPC:

- [Junos Address Aware on MS-MIC and MS-MPC on page 84](#)
- [Junos VPN Site Secure Support on the MS-MIC and MS-MPC on page 84](#)
- [Junos Traffic Vision Support on MS-MIC and MS-MPC on page 85](#)
- [Aggregated Multiservices \(AMS\) Interface Support on MS-MIC on page 85](#)

### Junos Address Aware on MS-MIC and MS-MPC

---

Junos OS Release 13.2 extends support for the Junos Address Aware technologies (previously referred to by the generic term NAT features) to the newly-introduced Multiservices MIC and Multiservices MPC on MX Series routers. Because the Junos OS extension-provider packages come preinstalled and preconfigured on the MS-MIC and MS-MPC, you do not need to explicitly configure the **The adaptive-services** configuration at the **[edit chassis fpc number pic number adaptive-services]** hierarchy level.

The following Junos Address Aware features are supported on the MS-MIC and MS-MPC in Release 13.2:

- NAT44, Dynamic NAT44, and NAPT44.
- Random port allocation and round-robin address allocation for NAPT.



**NOTE:** Port block allocation (PBA), including secured port block allocation and deterministic NAT, are *not* supported.

- Address pooling paired (APP), endpoint-independent mapping (EIM), endpoint-independent filtering (EIF).
- For NAT44, Dynamic NAT44, and NAPT44, the following ALGs are supported: ICMP, TFTP, RSH, FTP, DNS, and RTSP ALG. However, RSH is not supported for NAPT.
- NAT64 with ICMP ALG.
- AMS support with N:1 and 1:1 (only for NAT44) high availability.

For more information on configuring Junos Address Aware on the MS-MIC and MS-MPC, see *Next-Generation Network Addressing Carrier-Grade NAT and IPv6 Solutions*. For additional information on configuring services interfaces, see the *Junos OS Services Interfaces Configuration Guide*.

### Junos VPN Site Secure Support on the MS-MIC and MS-MPC

---

Junos OS Release 13.2 extends support for Junos VPN Site Secure technologies (formerly known as IPsec features) to the newly-introduced Multiservices MIC and Multiservices MPC on MX Series routers. Because the Junos OS extension-provider packages come preinstalled and preconfigured on the MS-MIC and MS-MPC, you do not need to explicitly configure the **adaptive-services** configuration at the **[edit chassis fpc number pic number]** hierarchy level.

The following Junos VPN Site Secure features are supported on the MS-MIC and MS-MPC in Release 13.2:

- Dynamic End Points (DEP)
- Encapsulating Security Payload (ESP) protocol
- Dead Peer Detection (DPD) trigger messages
- Sequence Number Rollover notifications

However, in Junos OS, Release 13.2, the Junos VPN Site Secure support on the MS-MIC and MS-MPC is limited to IPv4 traffic.

For more information about configuring Junos VPN Site Secure on services interfaces, see [“Example: Configuring Junos VPN Site Secure on MS MIC and MS-MPC” on page 102](#).

### **Junos Traffic Vision Support on MS-MIC and MS-MPC**

Junos OS Release 13.2 extends Junos Traffic Vision (previously known as Jflow) version 9 support to the Multiservices MIC and Multiservices MPC on MX Series routers. Junos Traffic Vision support on the MS-MIC and MS-MPC enables you to keep track of the packets received on an MS-MIC or an MS-MPC and to generate flow records that contain information such as the source address of the packet, the destination address of the packet, packets and byte counts, and so on.

Starting with Release 13.2, the Junos OS extension-provider packages come preinstalled on the MS-MIC and MS-MPC. The **adaptive-services** configuration at the **[edit chassis fpc number pic number]** hierarchy level is preconfigured on these cards.

For more information on configuring Junos Traffic Vision on MS-MIC and MS-MPC, see [“Example: Configuring Flow Monitoring on MS-MIC and MS-MPC” on page 86](#).

### **Aggregated Multiservices (AMS) Interface Support on MS-MIC**

Junos OS Release 13.2 extends the aggregated multiservices (AMS) interfaces support to the Multiservices MIC (MS-MIC-16G) on MX Series routers. An AMS interface is a bundle of services interfaces among which you can load balance the services configured on a service set. The MS-MIC supports both interface style and next-hop style configurations. You can add up to eight MS-MICs to an AMS interface and associate the AMS interface with a service set. Note that all member interfaces of an AMS interface must be of the same interface type. That is, if you are adding an MS-MIC as a member interface of an AMS interface, all members must be MS-MICs.

Because there are multiple services interfaces that are configured as part of an AMS bundle, AMS configuration also provides for high availability and failover. You can either configure one of the member interfaces to be the backup interface that comes online when one of the active interfaces goes down, or configure the bundle in such a way that when a member interface goes down the traffic assigned to that member is shared across the remaining member interfaces.

For more information about AMS interfaces, see [“Understanding Aggregated Multiservices Interfaces” on page 93](#).

For more information about configuring an AMS interface and interface style configuration, see [“Example: Configuring an Aggregated Multiservices Interface \(AMS\)” on page 94](#).

For more information about configuring next-hop style configuration on an AMS, see [“Example: Configuring Next-Hop Style Services on an Aggregated Multiservices Interface” on page 99](#).

## Example: Configuring Flow Monitoring on MS-MIC and MS-MPC

This example shows how you can configure Junos Traffic Vision for flow monitoring on MS-MIC and MS-MPC, and contains the following sections:

- [Hardware and Software Requirements on page 86](#)
- [Junos Traffic Vision Support on MS-MIC and MS-MPC on page 86](#)
- [Configuring Flow Monitoring on MS-MIC on page 87](#)
- [Verification on page 92](#)

---

### Hardware and Software Requirements

This example requires an MX Series router that has:

- Junos OS Release 13.2 running on it.
- An MS-MIC installed in it.

---

### Junos Traffic Vision Support on MS-MIC and MS-MPC

Junos Traffic Vision (previously known as Jflow) is the accounting service that is available on the MS-MIC and MS-MPC. Junos Traffic Vision enables users to keep track of the packets received on the MS-MIC or MS-MPC and to generate flow records that contain information such as the source address of the packet, the destination address of the packet, packets and byte counts, and so on. Junos Traffic Vision implementation does not interrupt the traffic, instead it makes a copy of the incoming packet and sends that copy to the service interface card for analyzing the information and maintaining the record.

Starting with Release 13.2, the Junos OS extension-provider packages come preinstalled on a multiservices MIC and MPC (MS-MIC and MS-MPC). The **adaptive-services** configuration at the `[edit chassis fpc number pic number]` hierarchy level is preconfigured on these cards.

Before you configure Junos Traffic Vision on an MS-MIC or an MS-MPC, you must create a firewall filter that has **sample** configured as action, and apply that to the interface on which you want to monitor the traffic. The flow-collector in Junos Traffic Vision implementations is a device for collecting the flow records. The flow collector is typically deployed outside the network.



**NOTE:** For more information about configuring firewall filters, see the *Junos OS Firewall Filters Configuration Guide*.

---

On MS-MIC and MS-MPC, Junos OS supports Junos Traffic Vision Version 9 (v9). Junos Traffic Vision v9 supports sampling of IPv4, IPv6, and MPLS traffic. A services interface card is essential for the v9 implementation, and hence this is often known as PIC-based monitoring.

You can configure the maximum time for which the flow records are stored on the services interface card. The active timeout and inactive timeout values, configured while defining the template, control the export of flow records to the collector. An MS-MIC can store a maximum of 14 million flow records, whereas an MS-MPC can store up to 30 million flows per NPU.



**NOTE:** In Junos Traffic Vision configurations using the Junos OS extension-provider package, modifying the following statements after flow monitoring has been initiated causes all existing flows to expire:

- At the [edit forwarding-options sampling instance *instance-name* family (inet |inet6 |mpls) output] and [edit forwarding-options sampling family (inet |inet6 |mpls) output] hierarchy levels:
  - flow-server *ip-address*
  - flow-server port *port-number*
  - flow-server template *template*
- At the [edit services flow-monitoring version9 template *template-name* mpls-ipv4-template] and [edit services flow-monitoring version9 template *template-name* mpls-template] hierarchy levels:
  - label-position

Because these changes can disrupt the ongoing flow monitoring, we recommend that you do not change these values after flow monitoring has been initiated on a device. The changes made to these configuration statements when flow monitoring is going on, apply only to the newly created flows.

Also, note that these changes do not disrupt flow monitoring on devices running Jflow configuration using the Junos OS Layer 2 services package. However, even in the case of Layer 2 service package-based configuration, the changes are applied only to the newly created flows. The existing flows continue to use the initial settings.

### Configuring Flow Monitoring on MS-MIC

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.



**NOTE:** You can follow the same procedure and use the same configuration for configuring flow monitoring on MS-MPC.

**Enabling the Services  
Interface Card**

```
set interfaces ms-2/0/0 unit 0 family inet
```

**Configuring the  
Template and Timers**

```
set services flow-monitoring version9 template template1
set services flow-monitoring version9 template template1 flow-active-timeout 120
set services flow-monitoring version9 template template1 flow-inactive-timeout 60
set services flow-monitoring version9 template template1 ipv4-template
set services flow-monitoring version9 template template1 template-refresh-rate packets
    100
set services flow-monitoring version9 template template1 template-refresh-rate seconds
    600
set services flow-monitoring version9 template template1 option-refresh-rate packets
    100
set services flow-monitoring version9 template template1 option-refresh-rate seconds
    600
```

**Configuring Service Set  
Properties**

```
set services service-set ss1 jflow-rules sampling
set services service-set ss1 sampling-service service-interface ms-2/0/0.0
```

**Configuring  
Forwarding Options  
and Flow Server  
Settings**

```
set forwarding-options sampling input rate 10
set forwarding-options sampling input run-length 18
set forwarding-options sampling family inet output flow-server 10.44.4.3 port 1055
set forwarding-options sampling family inet output flow-server 10.44.4.3 version9
    template template1
set forwarding-options sampling family inet output interface ms-2/0/0.0 source-address
    101.78.22.1
```

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Configure the services interface.

```
[edit interfaces]
user@router1# set interfaces ms-2/0/0 unit 0 family inet
user@router1# set interfaces ms-2/0/0 unit 1 family inet6
user@router1# set interfaces ms-2/0/0 unit 2 family mpls
```

2. Configure the template properties and the export policy timers.

```
[edit services]
user@router1# set flow-monitoring version9 template template1
user@router1# set flow-monitoring version9 template template1 flow-active-timeout
    120
user@router1# set flow-monitoring version9 template template1 flow-inactive-timeout
    60
user@router1# set flow-monitoring version9 template template1 ipv4-template
user@router1# set flow-monitoring version9 template template1 template-refresh-rate
    packets 100
user@router1# set flow-monitoring version9 template template1 template-refresh-rate
    seconds 600
user@router1# set flow-monitoring version9 template template1 option-refresh-rate
    packets 100
user@router1# set flow-monitoring version9 template template1 option-refresh-rate
    seconds 600
```

Table 12: Quick Reference to Key Configuration Statements at This Hierarchy Level

Configuration Statement	Description
<b>flow-active-timeout</b>	Configures the interval (in seconds) after which an active flow is exported.  Range is 10 through 600 seconds, and the default value is 60 seconds.
<b>flow-inactive-timeout</b>	Configures the interval (in seconds) of inactivity after which a flow is marked inactive.  Range is 10 through 600 seconds, and the default value is 60 seconds.
<i>ipv4-template   ipv6-template   mpls-template   mpls-ipv4-template</i>	Specifies the type of traffic for which the template is used for.
<b>template-refresh-rate</b>	Specifies the template refresh rate either as number of packets (range is 1 through 480,000 and the default value is 4800) or in seconds (the range is 10 through 600 and the default is 60).  Because the communication between the flow generator and the flow collector is a one-way communication, the flow generator has to regularly send updates about template definitions to the flow collector. The value configured for this statement controls the frequency of such updates.
<b>option-refresh-rate</b>	Specifies the option refresh rate either as number of packets (range is 1 through 480,000 and the default value is 4800) or in seconds (the range is 10 through 600 and the default is 60).

## 3. Configure service set properties.

```
[edit services]
user@router1# set service-set ss1 jflow-rules sampling
user@router1# set service-set ss1 sampling-service service-interface ms-2/0/0.0
```

Table 13: Quick Reference to Configuration Statements at This Hierarchy Level

Configuration Statement	Description
<b>sampling</b>	Configures the service set to handle sampling/flow monitoring activities.
<b>service-interface</b>	Specifies the service interface associated with the service set.  The interface configured here should match the interface configured at the <b>[edit forwarding-options sampling family inet output]</b> . Also, note that the interface should not be associated with any other service set.

## 4. Configure forwarding options and flow-server properties.

```
[edit forwarding-options]
user@router1# set sampling input rate 10
user@router1# set sampling input run-length 18
user@router1# set sampling family inet output flow-server 10.44.4.3 port 1055
user@router1# set sampling family inet output flow-server 10.44.4.3 version9 template
template1
user@router1# set sampling family inet output interface ms-2/0/0.0 source-address
101.78.22.1
```



**NOTE:** You can specify the sampling parameters either at the global level (as shown in this example) or at the FPC level by defining a sampling instance. To define a sampling instance, include the instance statement at the [edit forwarding-options sampling] hierarchy level, and the sampling-instance statement at the [edit chassis fpc *number*] hierarchy level to associate the sampling instance with an FPC. Under the [edit forwarding-options sampling instance *instance*] hierarchy level, you must also include the input and output configurations explained in this step.

**Table 14: Quick Reference to Key Configuration Statements at this Hierarchy Level**

Configuration Statement	Description
<b>rate</b>	The ratio of the number of packets to be sampled. For example, if you specify a rate of 10, every tenth packet (1 packet out of 10) is sampled.  The range is 1 through 65,535.
<b>run-length</b>	The number of samples following the initial trigger event. This enables you to sample packets following those already being sampled.  The range is 0 through 20, and the default is 0.
<b>flow-server</b>	A host system to collect sampled flows using the version 9 format.
<b>source-address</b>	An IPv4 address to be used as the source address of the exported packet.

**Result** From the configuration mode, confirm your configuration by entering the **show chassis fpc 2**, **show interfaces**, and **show forwarding-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@router1# show interfaces
ms-2/0/0 {
  unit 0 {
    family inet;
  }
}
```

```
}
user@router1# show services
flow-monitoring {
  version9 {
    template template1 {
      flow-active-timeout 120;
      flow-inactive-timeout 60;
      template-refresh-rate {
        packets 100;
        seconds 600;
      }
      option-refresh-rate {
        packets 100;
        seconds 600;
      }
      ipv4-template;
    }
  }
}
service-set ssl {
  jflow-rules {
    sampling;
  }
  sampling-service {
    service-interface ms-2/0/0.0
  }
}

user@router1# show forwarding-options
sampling {
  input {
    rate 10;
    run-length 18;
  }
  family inet {
    output {
      flow-server 10.44.4.3 {
        port 1055;
        version9 {
          template {
            template1;
          }
        }
      }
    }
    interface ms-2/0/0.0 {
      source-address 101.78.22.1;
    }
  }
}
}
```

## Verification

---

Confirm that the configuration is working properly.

- [Verifying the Junos Traffic Vision Configuration on page 92](#)
- [Viewing the Flow Details on page 92](#)
- [Viewing Details of Errors That Occurred on the Services Interface on page 92](#)

### *Verifying the Junos Traffic Vision Configuration*

**Purpose** Verify that Junos Traffic Vision is enabled on the router.

**Action** From operational mode, enter the **show services accounting status** command.

```
user@router1> show services accounting status
Service Accounting interface: ms-2/0/0
Export format: 9, Route record count: 2093
IFL to SNMP index count: 35, AS count: 2
Configuration set: Yes, Route record set: Yes, IFL SNMP map set: Yes
```

**Meaning** Shows the service interface on which monitoring is configured, and also provides information about the export format used (version 9 in this case).

### *Viewing the Flow Details*

**Purpose** View the flow details on the interface configured for flow monitoring.

**Action** From operational mode, enter the **show services accounting flow** command.

```
user@router1> show services accounting flow
Flow information
Service Accounting interface: ms-2/0/0, Local interface index: 229
Flow packets: 220693, Flow bytes: 24276230
Flow packets 10-second rate: 99, Flow bytes 10-second rate: 10998
Active flows: 10, Total flows: 12
Flows exported: 199, Flows packets exported: 718
Flows inactive timed out: 2, Flows active timed out: 199
```

### *Viewing Details of Errors That Occurred on the Services Interface*

**Purpose** View details of errors, if any, on the interface that is configured for flow monitoring.

**Action** From operational mode, enter the **show services accounting errors** command.

```
user@router1> show services accounting errors
Error information
Service Accounting interface: ms-2/0/0
Service sets dropped: 0, Active timeout failures: 0
Export packet failures: 0, Flow creation failures: 0
Memory overload: No
```

## Understanding Aggregated Multiservices Interfaces

This topic contains the following sections:

- [Aggregated Multiservices Interface on page 93](#)
- [Member Failure Options and High Availability Settings on page 93](#)

### Aggregated Multiservices Interface

In Junos OS, you can combine multiple services interfaces to create a bundle of interfaces that can function as a single interface. Such a bundle of interfaces is known as an aggregated multiservices interface (AMS), and is denoted as `amsN` in the configuration, where *N* is a unique number that identifies an AMS interface (for example, `ams0`).

AMS configuration provides higher scalability, improved performance, and better failover and load-balancing options.

The current service set configuration model in Junos OS supports only one service PIC per service set. All services provisioned using a service set must be handled by the only one service PIC associated with that service set. AMS configuration enables you to address this limitation by associating an AMS bundle with a service set. An AMS bundle can have up to eight services PICs as member interfaces and can distribute services among the member interfaces. This allows you to have multiple service interfaces to handle services configured in one service set.



**NOTE:** Member interfaces are identified as `mams` in the configuration. The `chassisd` process in routers that support AMS configuration creates a `mams` entry each for every multiservices interface on the router.



**NOTE:** You cannot include MS-DPCs or other multiservices PICs in an AMS configuration that contains MS-MICs or MS-MPCs as member interfaces.

By default, the traffic distribution over the member interfaces of an AMS interface happens in a round-robin fashion. You can also configure the following hash key values to regulate the traffic distribution: **source-ip**, **destination-ip**, **iif** (incoming interface), **oif** (outgoing interface), and **protocol**. For services that require traffic symmetry, you must configure symmetrical hashing. Symmetrical hashing configuration ensures that both forward and reverse traffic are routed through the same member interface.



**NOTE:** Junos OS AMS configuration supports only IPv4 traffic.

### Member Failure Options and High Availability Settings

Because multiple service interfaces are configured as part of an AMS bundle, AMS configuration also provides for failover and high availability support. You can either configure one of the member interfaces as a backup interface that becomes active when

any one of the other member interfaces goes down, or configure the AMS in such a way that when one of the member interfaces goes down, the traffic assigned to that interface is shared across the active interfaces.

The **member-failure-options** configuration statement enables you to configure how to handle traffic when a member interface fails. One option is to redistribute the traffic immediately among the other member interfaces. However, redistribution of traffic involves recalculating the hash tags, and might cause some disruption in traffic on all the member interfaces.

The other option is to configure the AMS to drop all traffic that is assigned to the failed member interface. With this you can optionally configure an interval, **rejoin-timeout**, for the AMS to wait for the failed interface to come back online after which the AMS can redistribute the traffic among other member interfaces. If the failed member interface comes back online before the configured wait time, traffic continues unaffected on all member interfaces, including the interface that has come back online and resumed the operations.

You can also control the rejoining of the failed interface when it comes back online. If you do not include the **enable-rejoin** statement in the **member-failure-options** configuration, the failed interface is not allowed to rejoin the AMS when it comes back online. In such cases, you can manually rejoin that to the AMS by executing the **request interfaces revert interface-name** operational mode command.

The **rejoin-timeout** and **enable-rejoin** statements enable you to minimize traffic disruptions when member interfaces flap.



**NOTE:** When **member-failure-options** are not configured, the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

---

The **high-availability-options** configuration enables you to designate one of the member interfaces as a backup interface. The backup interface does not participate in routing operations as long as it remains a backup interface. When a member interface fails, the backup interface handles the traffic assigned to the failed interface. When the failed interface comes back online, it becomes the new backup interface.

When both **member-failure-options** and **high-availability-options** are configured for an AMS, the **high-availability-options** configuration takes precedence over the **member-failure-options** configuration. If a second failure occurs before the failed interface comes back online to be the new backup, the **member-failure-options** configuration comes into effect.

### Example: Configuring an Aggregated Multiservices Interface (AMS)

- [Hardware and Software Requirements on page 95](#)
- [Overview on page 95](#)
- [Configuration on page 95](#)
- [Verification on page 99](#)

## Hardware and Software Requirements

This example requires MX Series routers that have services interfaces installed in that and Junos OS Release 13.2 running on that.

## Overview

The aggregated multiservices (AMS) interface configuration in Junos OS enables you to combine multiple services interfaces to create a bundle of interfaces that can function as a single interface. This example shows you how to configure an AMS interface, load-balancing options, member failure options, high availability settings on an AMS interface, and an interface-style service set configuration that uses the AMS interface.



**NOTE:** You cannot include MS-DPCs or other multiservices PICs in an AMS configuration that contains MS-MICs or MS-MPCs as member interfaces.

For more information about AMS interfaces, see [“Understanding Aggregated Multiservices Interfaces” on page 93](#).

## Configuration

<b>CLI Quick Configuration</b>	To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.
<b>Adding Member Interfaces</b>	<pre>set interfaces ams0 load-balancing-options member-interface mams-0/0/0 set interfaces ams0 load-balancing-options member-interface mams-0/1/0 set interfaces ams0 load-balancing-options member-interface mams-1/0/0 set interfaces ams0 load-balancing-options member-interface mams-1/1/0 set interfaces ams0 load-balancing-options member-interface mams-2/0/0 set interfaces ams0 load-balancing-options member-interface mams-2/1/0</pre>
<b>Configuring Logical Units</b>	<pre>set interfaces ams0 unit 1 family inet</pre>
<b>Configuring Member Failure Options</b>	<pre>set interfaces ams0 load-balancing-options member-failure-options drop-member-traffic   rejoin-timeout 300 set interfaces ams0 load-balancing-options member-failure-options drop-member-traffic   enable-rejoin</pre>
<b>Configuring High Availability Options</b>	<pre>set interfaces ams0 load-balancing-options high-availability-options many-to-one   preferred-backup mams-1/0/0</pre>
<b>Configuring Service Set and Interface Services</b>	<pre>set services service-set ams-ss1 interface-service service-interface ams0.1 set services service-set ams-ss1 interface-service load-balancing-options hash-keys   ingress-key source-ip set services service-set ams-ss1 interface-service load-balancing-options hash-keys   egress-key destination-ip</pre>

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Create an aggregated multiservices interface and add member interfaces.



**NOTE:** You cannot configure the same mams to be part of two different AMS interfaces at the same time.

```
[edit]
user@router1# set interfaces ams0 load-balancing-options member-interface
mams-0/0/0
user@router1# set interfaces ams0 load-balancing-options member-interface
mams-0/1/0
user@router1# set interfaces ams0 load-balancing-options member-interface
mams-1/0/0
user@router1# set interfaces ams0 load-balancing-options member-interface
mams-1/1/0
user@router1# set interfaces ams0 load-balancing-options member-interface
mams-2/0/0
user@router1# set interfaces ams0 load-balancing-options member-interface
mams-2/1/0
```

2. Configure logical units for the AMS interface.



**NOTE:** An AMS interface and its member interfaces cannot share the same logical interface units. For example, if one of the member interfaces has logical units 1 and 2 configured on it, you cannot configure logical units 1 and 2 for the AMS. Similarly, if you have configured logical units 3 and 4 on the AMS, you cannot configure those units on any of the member interfaces.

```
[edit interfaces]
user@router1# set ams0 unit 1 family inet
```

3. Configure member failure options.

```
[edit interfaces ams0]
user@router1# set load-balancing-options member-failure-options
drop-member-traffic rejoin-timeout 300
user@router1# set load-balancing-options member-failure-options
drop-member-traffic enable-rejoin
```



**NOTE:** This example shows the `drop-member-traffic` configuration. However, if you would like to redistribute the traffic to other available members when one of the member interfaces goes down, you can include the `redistribute-all-traffic` statement instead of the `drop-member-traffic` statement.

The default behavior, when the `member-failure-options` configuration is not included, is to drop member traffic with a rejoin timeout of 120 seconds.

4. Configure the high-availability options.

```
[edit interfaces ams0]
user@router1# set load-balancing-options high-availability-options many-to-one
preferred-backup mams-1/0/0
```

5. Configure interface style services.

```
[edit services]
user@router1# set service-set ams-ss1 interface-service service-interface ams0.1
user@router1# set service-set ams-ss1 interface-service load-balancing-options
hash-keys ingress-key source-ip
user@router1# set service-set ams-ss1 interface-service load-balancing-options
hash-keys egress-key destination-ip
```

6. If you are done configuring the device, commit the configuration.

```
[edit]
user@router1# commit
```

**Table 15: Key Configuration Statements Used in this Example**

Statement	Description
<b>member-interface</b>	Adds a member interface (mams) to the AMS bundle.
<b>drop-member-traffic</b>	Specifies that all traffic to a member be dropped in case the member interface fails.
<b>rejoin-timeout</b>	Specifies the time interval, in seconds, for the AMS to wait before declaring a member interface down. If the failed member comes back online during this period, it can rejoin the AMS and resume traffic forwarding.  The range is 0 through 1000 seconds.
<b>enable-rejoin</b>	Specifies whether a failed interface be allowed to rejoin the AMS when it comes back online.  If this statement is not included in the configuration, you must manually add the interface to the AMS when the interface is back online.
<b>preferred-backup</b>	Designates a member interface as the floating backup.

Table 15: Key Configuration Statements Used in this Example (*continued*)

Statement	Description
<b>interface-services</b>	Specifies a service interface, an AMS interface in this example, to handle interface services.
<b>hash-keys</b>	<p>Specifies the load-balancing hash keys. You can configure the following hash key values: <b>source-ip</b>, <b>destination-ip</b>, <b>iif</b> (incoming interface), <b>oif</b> (outgoing interface), and <b>protocol</b>.</p> <p><b>NOTE:</b> For services that require traffic symmetry, you must configure symmetrical hashing. Symmetrical hashing configuration ensures that both forward and reverse traffic are routed through the same member interface.</p>

**Results** From the configuration mode, confirm your configuration by entering the **show interfaces ams0** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

user@router1# show interfaces ams0
load-balancing-options {
  member-interface mams-0/0/0;
  member-interface mams-0/1/0;
  member-interface mams-1/0/0;
  member-interface mams-1/1/0;
  member-interface mams-2/0/0;
  member-interface mams-2/1/0;
  member-failure-options {
    drop-member-traffic {
      rejoin-timeout 300;
      enable-rejoin;
    }
  }
  high-availability-options {
    many-to-one {
      preferred-backup mams-1/0/0;
    }
  }
}
unit 1 {
  family inet;
}

user@router1# show services
service-set ams-ssl {
  interface-service {
    service-interface ams0.1;
    load-balancing-options {
      hash-keys {
        ingress-key source-ip;
        egress-key destination-ip;
      }
    }
  }
}

```

```
}

```

### Verification

Confirm that the configuration is working properly.

- [Verifying the AMS Configuration on page 99](#)

#### Verifying the AMS Configuration

**Purpose** Verify the AMS configuration and status of member interfaces.

**Action** From operational mode, enter the **show** command.

```
user@router1> show interfaces load-balancing detail
Load-balancing interfaces detail
Interface      : ams0
State          : Up
Last change    : 00:01:28
Member count   : 6
HA Model       : Many-to-One
Members       :
  Interface    Weight  State
  mams-0/0/0   10      Active
  mams-0/1/0   10      Active
  mams-1/0/0   10      Backup
  mams-1/1/0   10      Active
  mams-2/0/0   10      Active
  mams-2/1/0   10      Active
```

**Meaning** Shows that **ams0** has six member interfaces with a many-to-one backup configuration. Of the six member interfaces, five are in active state and one, mams-1/0/0, is in backup state.

## Example: Configuring Next-Hop Style Services on an Aggregated Multiservices Interface

- [Hardware and Software Requirements on page 99](#)
- [Overview on page 99](#)
- [Configuration on page 100](#)

### Hardware and Software Requirements

MX Series routers with services interfaces installed and running Junos OS Release 13.2.

### Overview

Starting with Release 13.2, Junos OS extends next-hop style services support to aggregated multiservices (AMS) interfaces. In releases earlier than 12.3, only interface style services configurations were supported on AMS interfaces.

The next-hop style services configuration on AMS interfaces is different from the interface style services configuration. For next-hop style services, the load-balancing hash keys are defined as part of the logical unit configuration of the AMS interface. For interface style services, the hash keys configuration falls under the service-set configuration.

This example explains the next-hop style services configuration on an AMS interface, and shows the verification steps to verify that the configuration is working correctly.

### Configuration

---

<b>CLI Quick Configuration</b>	To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.
<b>Configuring an aggregated multiservices interface</b>	<pre>set interfaces ams0 load-balancing-options member-interface mams-1/0/0 set interfaces ams0 load-balancing-options member-interface mams-1/1/0 set interfaces ams0 load-balancing-options member-interface mams-2/0/0 set interfaces ams0 load-balancing-options member-interface mams-2/1/0 set interfaces ams0 unit 1 family inet set interfaces ams0 unit 1 service-domain inside set interfaces ams0 unit 2 family inet set interfaces ams0 unit 2 service-domain outside</pre>
<b>Configuring Routing Instances that Use AMS interfaces</b>	<pre>set routing-instances ri-internal instance-type virtual-router set routing-instances ri-internal interface ge-0/0/2.0 set routing-instances ri-internal interface ams0.1 set routing-instances ri-internal routing-options static route 22.22.22.0/24 next-hop ams0.1 set routing-instances ri-external instance-type virtual-router set routing-instances ri-external interface ge-2/0/6.0 set routing-instances ri-external interface ams0.2 set routing-instances ri-external routing-options static route 0.0.0.0/0 next-hop ams0.2</pre>
<b>Configuring Hash Keys</b>	<pre>set interfaces ams0 unit 1 load-balancing-options hash-keys ingress-key source-ip protocol set interfaces ams0 unit 2 load-balancing-options hash-keys ingress-key destination-ip protocol</pre>
<b>Configure Next Hop Services</b>	<pre>set services service-set ams-test stateful-firewall-rules sfw1 set services service-set ams-test next-hop-service inside-service-interface ams0.1 set services service-set ams-test next-hop-service outside-service-interface ams0.2</pre>

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see “*Using the CLI Editor in Configuration Mode*” in the *CLI User Guide*.

1. Configure an aggregated multiservices interface and the load-balancing options.

```
[edit interfaces ams0]
user@router1# set load-balancing-options member-interface mams-1/0/0
user@router1# set load-balancing-options member-interface mams-1/1/0
user@router1# set load-balancing-options member-interface mams-2/0/0
user@router1# set load-balancing-options member-interface mams-2/1/0
user@router1# set unit 1 family inet
user@router1# set unit 1 service-domain inside
user@router1# set unit 2 family inet
user@router1# set unit 2 service-domain outside
```

2. Configure routing instances that use the aggregated multiservices interfaces configured in the first step.

```
[edit routing-instances]
user@router1# set ri-internal instance-type virtual-router
user@router1# set ri-internal interface ge-0/0/2.0
user@router1# set ri-internal interface ams0.1
user@router1# set ri-internal routing-options static route 22.22.22.0/24 next-hop
  ams0.1
user@router1# set ri-external instance-type virtual-router
user@router1# set ri-external interface ge-2/0/6.0
user@router1# set ri-external interface ams0.2
user@router1# set ri-external routing-options static route 0.0.0.0/0 next-hop ams0.2
```

3. Configure hash keys for the aggregated multiservices interfaces.



**NOTE:** Unlike in the interface-style configuration where hash keys are defined in the service-set configuration, for next-hop services, the hash keys are specified in the AMS configuration under the logical units.

```
[edit interfaces ams0]
user@router1# set unit 1 load-balancing-options hash-keys ingress-key source-ip
  protocol
user@router1# set unit 2 load-balancing-options hash-keys ingress-key destination-ip
  protocol
```

4. Configure next-hop style services under the service-set configuration.

```
[edit services service-set ams-test]
user@router1# set stateful-firewall-rules sfw1
user@router1# set next-hop-service inside-service-interface ams0.1
user@router1# set next-hop-service outside-service-interface ams0.2
```

5. Commit the configuration.

```
[edit]
user@router1# commit
```

**Results** From the configuration mode, confirm your configuration by entering the **show interfaces ams0**, **show routing-instances**, and **show services service-set ams-test** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@router1# show interfaces ams0
load-balancing-options {
  member-interface mams-1/0/0;
  member-interface mams-1/1/0;
  member-interface mams-2/0/0;
  member-interface mams-2/1/0;
  member-failure-options {
    redistribute-all-traffic {
      enable-rejoin;
    }
  }
}
unit 1 {
  family inet;
  service-domain inside;
```

```

        load-balancing-options {
            hash-keys {
                ingress-key [ source-ip protocol ];
            }
        }
    }
    unit 2 {
        family inet;
        service-domain outside;
        load-balancing-options {
            hash-keys {
                ingress-key [ destination-ip protocol ];
            }
        }
    }
}

user@router1# show routing-instances
ri-internal {
    instance-type virtual-router;
    interface ge-0/0/2.0;
    interface ams0.1
    routing-options {
        static {
            route 22.22.22.0/24 next-hop ams0.1;
        }
    }
}
ri-external {
    instance-type virtual-router;
    interface ge-2/0/6.0;
    interface ams0.2
    routing-options {
        static {
            route 0.0.0.0/0 next-hop ams0.2;
        }
    }
}

user@router1# show services service-set ams
stateful-firewall-rules sfw1;
next-hop-service {
    inside-service-interface ams0.1;
    outside-service-interface ams0.2;
}

```

### Example: Configuring Junos VPN Site Secure on MS MIC and MS-MPC



**NOTE:** You can follow the same procedure and use the same configuration given in this example, to configure Junos VPN Site Secure (previously known as IPsec features) on MS-MPCs.

This example contains the following sections:

- [Requirements on page 103](#)
- [Overview on page 103](#)
- [Configuration on page 104](#)
- [Verification on page 111](#)

## Requirements

This example uses the following hardware and software components:

- Two MX Series routers with MS-MICs
- Junos OS Release 13.2 or later

## Overview

Junos OS, Release 13.2, extends support for Junos VPN Site Secure (formerly known as IPsec features) to the newly-introduced Multiservices MIC and MPC (MS-MIC and MS-MPC) on MX Series routers. The Junos OS extension-provider packages come preinstalled and preconfigured on the MS-MIC and MS-MPC.

The following Junos VPN Site Secure features are supported on the MS-MIC and MS-MPC in Release 13.2:

- Dynamic End Points (DEP)
- Encapsulating Security Payload (ESP) protocol
- Dead Peer Detection (DPD) trigger messages
- Sequence Number Rollover notifications
- Static IPsec tunnels with next-hop-style and interface-style service sets

However, in Junos OS, Release 13.2, the Junos VPN Site Secure support on the MS-MIC and MS-MPC is limited to IPv4 traffic.

This example shows configuration of two routers, Router 1 and Router 2, that have an IPsec VPN tunnel configured between them.

While configuring the routers, note the following points:

- The IP address you configure for **source-address** under the **[edit services ipsec-vpn rule *name* term *term* from]** hierarchy level on Router 1 must be the same as the IP address you configure for **destination-address** under the same hierarchy on Router 2, and vice versa.
- The IP address of the **remote-gateway** you configure under the **[edit services ipsec-vpn rule *name* term *term* then]** hierarchy level should match the IP address of the **local-gateway** you configure under the **[edit services service-set *name* ipsec-vpn-options]** hierarchy level of Router 2, and vice versa.

## Configuration

This section contains:

- [Configuring Router 1 on page 106](#)
- [Configuring Router 2 on page 108](#)

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

#### Configuring Interfaces on Router 1

```
set interfaces ms-4/0/0 unit 0 family inet
set interfaces ms-4/0/0 unit 1 family inet
set interfaces ms-4/0/0 unit 1 family inet6
set interfaces ms-4/0/0 unit 1 service-domain inside
set interfaces ms-4/0/0 unit 2 family inet
set interfaces ms-4/0/0 unit 2 family inet6
set interfaces ms-4/0/0 unit 2 service-domain outside
set interfaces xe-0/2/0 unit 0 family inet address 10.0.1.1/30
```

#### Configuring IPsec VPN Service on Router 1

```
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 from source-address
  30.0.0.0/16
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 from destination-address
  80.0.0.0/16
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then remote-gateway 10.0.1.2
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then dynamic ike-policy
  ike_policy_ms_4_0_0
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then dynamic ipsec-policy
  ipsec_policy_ms_4_0_0
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then anti-replay-window-size
  4096
set services ipsec-vpn rule vpn_rule_ms_4_0_01 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0 protocol esp
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0 authentication-algorithm
  hmac-sha1-96
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0 encryption-algorithm
  3des-cbc
set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0 perfect-forward-secrecy keys
  group2
set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0 proposals
  ipsec_proposal_ms_4_0_0
set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0 authentication-method
  pre-shared-keys
set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0 dh-group group2
set services ipsec-vpn ike policy ike_policy_ms_4_0_0 version 2
set services ipsec-vpn ike policy ike_policy_ms_4_0_0 proposals ike_proposal_ms_4_0_0
set services ipsec-vpn ike policy ike_policy_ms_4_0_0 pre-shared-key ascii-text secret-data
```

#### Configuring a Service Set on Router 1

```
set services service-set ipsec_ss_ms_4_0_01 next-hop-service inside-service-interface
  ms-4/0/0.1
set services service-set ipsec_ss_ms_4_0_01 next-hop-service outside-service-interface
  ms-4/0/0.2
set services service-set ipsec_ss_ms_4_0_01 ipsec-vpn-options local-gateway 10.0.1.1
```

	set services service-set ipsec_ss_ms_4_0_01 ipsec-vpn-rules vpn_rule_ms_4_0_01
Configuring Routing Options on Router 1	set routing-options static route 80.0.0.0/16 next-hop ms-4/0/0.1
Configuring Interfaces on Router 2	set interfaces ms-1/0/0 unit 0 family inet set interfaces ms-1/0/0 unit 1 family inet set interfaces ms-1/0/0 unit 1 family inet6 set interfaces ms-1/0/0 unit 1 service-domain inside set interfaces ms-1/0/0 unit 2 family inet set interfaces ms-1/0/0 unit 2 family inet6 set interfaces ms-1/0/0 unit 2 service-domain outside set interfaces ge-2/0/0 unit 0 family inet address 10.0.1.2/30
Configuring IPsec VPN Service on Router 2	set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 from source-address 80.0.0.0/16 set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 from destination-address 30.0.0.0/16 set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then remote-gateway 10.0.1.1 set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then dynamic ike-policy ike_policy_ms_5_2_0 set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then dynamic ipsec-policy ipsec_policy_ms_5_2_0 set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then anti-replay-window-size 4096 set services ipsec-vpn rule vpn_rule_ms_5_2_01 match-direction input set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0 protocol esp set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0 authentication-algorithm hmac-sha1-96 set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0 encryption-algorithm 3des-cbc set services ipsec-vpn ipsec policy ipsec_policy_ms_5_2_0 perfect-forward-secrecy keys group2 set services ipsec-vpn ipsec policy ipsec_policy_ms_5_2_0 proposals ipsec_proposal_ms_5_2_0 set services ipsec-vpn ike proposal ike_proposal_ms_5_2_0 authentication-method pre-shared-keys set services ipsec-vpn ike proposal ike_proposal_ms_5_2_0 dh-group group2 set services ipsec-vpn ike policy ike_policy_ms_5_2_0 version 2 set services ipsec-vpn ike policy ike_policy_ms_5_2_0 proposals ike_proposal_ms_5_2_0 set services ipsec-vpn ike policy ike_policy_ms_5_2_0 pre-shared-key ascii-text <i>secret-data</i> set services ipsec-vpn establish-tunnels immediately
Configuring a Service Set on Router 2	set services service-set ipsec_ss_ms_5_2_01 next-hop-service inside-service-interface ms-1/0/0.1 set services service-set ipsec_ss_ms_5_2_01 next-hop-service outside-service-interface ms-1/0/0.2 set services service-set ipsec_ss_ms_5_2_01 ipsec-vpn-options local-gateway 10.0.1.2 set services service-set ipsec_ss_ms_5_2_01 ipsec-vpn-rules vpn_rule_ms_5_2_01
Configuring Routing Options on Router 2	set routing-options static route 30.0.0.0/16 next-hop ms-1/0/0.1

### Configuring Router 1

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.



**NOTE:** Starting with Release 13.2, the Junos OS extension-provider packages come preinstalled on multiservices MICs and MPCs (MS-MICs and MS-MPCs). The adaptive-services configuration at the [edit chassis fpc number pic number] hierarchy level is preconfigured on these cards.

1. Configure the interface properties.

```
user@router1# set interfaces ms-4/0/0 unit 0 family inet
user@router1# set interfaces ms-4/0/0 unit 1 family inet
user@router1# set interfaces ms-4/0/0 unit 1 family inet6
user@router1# set interfaces ms-4/0/0 unit 1 service-domain inside
user@router1# set interfaces ms-4/0/0 unit 2 family inet
user@router1# set interfaces ms-4/0/0 unit 2 family inet6
user@router1# set interfaces ms-4/0/0 unit 2 service-domain outside
user@router1# set interfaces xe-0/2/0 unit 0 family inet address 10.0.1.1/30
```

2. Configure IPsec properties.

```
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 from
source-address 30.0.0.0/16
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 from
destination-address 80.0.0.0/16
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then
remote-gateway 10.0.1.2
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then
dynamic ike-policy ike_policy_ms_4_0_0
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then
dynamic ipsec-policy ipsec_policy_ms_4_0_0
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then
anti-replay-window-size 4096
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 match-direction
input
user@router1# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0
protocol esp
user@router1# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0
authentication-algorithm hmac-sha1-96
user@router1# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0
encryption-algorithm 3des-cbc
user@router1# set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0
perfect-forward-secrecy keys group2
user@router1# set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0 proposals
ipsec_proposal_ms_4_0_0
user@router1# set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0
authentication-method pre-shared-keys
user@router1# set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0 dh-group
group2
user@router1# set services ipsec-vpn ike policy ike_policy_ms_4_0_0 version 2
```

```

user@router1# set services ipsec-vpn ike policy ike_policy_ms_4_0_0 proposals
ike_proposal_ms_4_0_0
user@router1# set services ipsec-vpn ike policy ike_policy_ms_4_0_0 pre-shared-key
ascii-text secret-key

```

3. Configure a service set.

```

user@router1# set services service-set ipsec_ss_ms_4_0_01 next-hop-service
inside-service-interface ms-4/0/0.1
user@router1# set services service-set ipsec_ss_ms_4_0_01 next-hop-service
outside-service-interface ms-4/0/0.2
user@router1# set services service-set ipsec_ss_ms_4_0_01 ipsec-vpn-options
local-gateway 10.0.1.1
user@router1# set services service-set ipsec_ss_ms_4_0_01 ipsec-vpn-rules
vpn_rule_ms_4_0_01

```

4. Configure routing options.

```

user@router1# set routing-options static route 80.0.0.0/16 next-hop ms-4/0/0.1

```

**Results** From the configuration mode of Router 1, confirm your configuration by entering the **show interfaces**, **show services ipsec-vpn**, and **show services service-set** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

user@router1# show interfaces
ms-4/0/0 {
  unit 0 {
    family inet;
  }
  unit 1 {
    family inet;
    family inet6;
    service-domain inside;
  }
  unit 2 {
    family inet;
    family inet6;
    service-domain outside;
  }
}
xe-0/2/0 {
  unit 0 {
    family inet {
      address 10.0.1.1/30;
    }
  }
}

user@router1# show services ipsec-vpn
rule vpn_rule_ms_4_0_01 {
  term term11 {
    from {
      source-address {
        30.0.0.0/16;
      }
      destination-address {

```

```

        80.0.0.0/16;
    }
}
then {
    remote-gateway 10.0.1.2;
    dynamic {
        ike-policy ike_policy_ms_4_0_0;
        ipsec-policy ipsec_policy_ms_4_0_0;
    }
    anti-replay-window-size 4096;
}
}
match-direction input;
}
ipsec {
    proposal ipsec_proposal_ms_4_0_0 {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
    }
    policy ipsec_policy_ms_4_0_0 {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals ipsec_proposal_ms_4_0_0;
    }
}
ike {
    proposal ike_proposal_ms_4_0_0 {
        authentication-method pre-shared-keys;
        dh-group group2;
    }
    policy ike_policy_ms_4_0_0 {
        version 2;
        proposals ike_proposal_ms_4_0_0;
        pre-shared-key ascii-text "$9$-tbYoDi.z39JG39ApREdb$"; ## SECRET-DATA
    }
}

user@router1# show services service-set
ipsec_ss_ms_4_0_01 {
    next-hop-service {
        inside-service-interface ms-4/0/0.1;
        outside-service-interface ms-4/0/0.2;
    }
    ipsec-vpn-options {
        local-gateway 10.0.1.1;
    }
    ipsec-vpn-rules vpn_rule_ms_4_0_01;
}

```

### Configuring Router 2

#### Step-by-Step Procedure

1. Configure the interfaces.  

```

user@router2# set interfaces ms-1/0/0 services-options inactivity-non-tcp-timeout
600

```

```

user@router2# set interfaces ms-1/0/0 unit 0 family inet
user@router2# set interfaces ms-1/0/0 unit 1 family inet
user@router2# set interfaces ms-1/0/0 unit 1 family inet6
user@router2# set interfaces ms-1/0/0 unit 1 service-domain inside
user@router2# set interfaces ms-1/0/0 unit 2 family inet
user@router2# set interfaces ms-1/0/0 unit 2 family inet6
user@router2# set interfaces ms-1/0/0 unit 2 service-domain outside
user@router2# set interfaces ge-2/0/0 unit 0 family inet address 10.0.1.2/30

```

2. Configure IPsec properties.

```

user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 from
source-address 80.0.0.0/16
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 from
destination-address 30.0.0.0/16
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then
remote-gateway 10.0.1.1
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then
dynamic ike-policy ike_policy_ms_5_2_0
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then
dynamic ipsec-policy ipsec_policy_ms_5_2_0
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then
anti-replay-window-size 4096
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 match-direction
input
user@router2# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0
protocol esp
user@router2# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0
authentication-algorithm hmac-sha1-96
user@router2# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0
encryption-algorithm 3des-cbc
user@router2# set services ipsec-vpn ipsec policy ipsec_policy_ms_5_2_0
perfect-forward-secrecy keys group2
user@router2# set services ipsec-vpn ipsec policy ipsec_policy_ms_5_2_0 proposals
ipsec_proposal_ms_5_2_0
user@router2# set services ipsec-vpn ike proposal ike_proposal_ms_5_2_0
authentication-method pre-shared-keys
user@router2# set services ipsec-vpn ike proposal ike_proposal_ms_5_2_0 dh-group
group2
user@router2# set services ipsec-vpn ike policy ike_policy_ms_5_2_0 version 2
user@router2# set services ipsec-vpn ike policy ike_policy_ms_5_2_0 proposals
ike_proposal_ms_5_2_0
user@router2# set services ipsec-vpn ike policy ike_policy_ms_5_2_0 pre-shared-key
ascii-text "$9$jokmT69pRhrz3hrev7Nik."
user@router2# set services ipsec-vpn establish-tunnels immediately

```

3. Configure a service set.

```

user@router2# set services service-set ipsec_ss_ms_5_2_01 next-hop-service
inside-service-interface ms-1/0/0.1
user@router2# set services service-set ipsec_ss_ms_5_2_01 next-hop-service
outside-service-interface ms-1/0/0.2
user@router2# set services service-set ipsec_ss_ms_5_2_01 ipsec-vpn-options
local-gateway 10.0.1.2
user@router2# set services service-set ipsec_ss_ms_5_2_01 ipsec-vpn-rules
vpn_rule_ms_5_2_01

```

4. Configure routing options.

```
user@router2# set routing-options static route 30.0.0.0/16 next-hop ms-1/0/0.1
```

**Results** From the configuration mode of Router 2, confirm your configuration by entering the **show interfaces**, **show services ipsec-vpn**, and **show services service-set** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@router2# show interfaces
ms-1/0/0 {
  unit 0 {
    family inet;
  }
  unit 1 {
    family inet;
    family inet6;
    service-domain inside;
  }
  unit 2 {
    family inet;
    family inet6;
    service-domain outside;
  }
}
ge-2/0/0 {
  unit 0 {
    family inet {
      address 10.0.1.2/30;
    }
  }
}

user@router2# show services ipsec-vpn
rule vpn_rule_ms_5_2_01 {
  term term11 {
    from {
      source-address {
        80.0.0.0/16;
      }
      destination-address {
        30.0.0.0/16;
      }
    }
    then {
      remote-gateway 10.0.1.1;
      dynamic {
        ike-policy ike_policy_ms_5_2_0;
        ipsec-policy ipsec_policy_ms_5_2_0;
      }
      anti-replay-window-size 4096;
    }
  }
  match-direction input;
}
ipsec {
```

```

proposal ipsec_proposal_ms_5_2_0 {
  protocol esp;
  authentication-algorithm hmac-sha1-96;
  encryption-algorithm 3des-cbc;
}
policy ipsec_policy_ms_5_2_0 {
  perfect-forward-secrecy {
    keys group2;
  }
  proposals ipsec_proposal_ms_5_2_0;
}
}
ike {
  proposal ike_proposal_ms_5_2_0 {
    authentication-method pre-shared-keys;
    dh-group group2;
  }
  policy ike_policy_ms_5_2_0 {
    version 2;
    proposals ike_proposal_ms_5_2_0;
    pre-shared-key ascii-text "$9$jokmT69pRhrz3hrev7Nik."; ## SECRET-DATA
  }
}
establish-tunnels immediately;

user@router2# show services service-set
ipsec_ss_ms_5_2_01 {
  next-hop-service {
    inside-service-interface ms-1/0/0.1;
    outside-service-interface ms-1/0/0.2;
  }
  ipsec-vpn-options {
    local-gateway 10.0.1.2;
  }
  ipsec-vpn-rules vpn_rule_ms_5_2_01;
}

user@router2 #show routing-options
static {
  route 30.0.0.0/16 next-hop ms-1/0/0.1;
}

```

### Verification

- [Verifying Tunnel Creation on page 111](#)
- [Verifying Traffic Flow Through the DEP Tunnel on page 112](#)
- [Verifying IPsec Security Associations for the Service Set on page 113](#)

### Verifying Tunnel Creation

**Purpose** Verify that Dynamic End Points are created.

**Action** Run the following command on Router 1:

```
user@router1 >show services ipsec-vpn ipsec security-associations detail
Service set: ipsec_ss_ms_4_0_01, IKE Routing-instance: default

Rule: vpn_rule_ms_4_0_01, Term: term11, Tunnel index: 1
Local gateway: 10.0.1.1, Remote gateway: 10.0.1.2
IPSec inside interface: ms-4/0/0.1, Tunnel MTU: 1500
Local identity: ipv4_subnet(any:0,[0..7]=30.0.0.0/16)
Remote identity: ipv4_subnet(any:0,[0..7]=80.0.0.0/16)

Direction: inbound, SPI: 112014862, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 24556 seconds
Hard lifetime: Expires in 25130 seconds
Anti-replay service: Enabled, Replay window size: 4096

Direction: outbound, SPI: 1469281276, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 24556 seconds
Hard lifetime: Expires in 25130 seconds
Anti-replay service: Enabled, Replay window size: 4096
```

**Meaning** The output shows that the IPSec SAs are up on the router with their state as Installed. The IPSec tunnel is up and ready to send traffic over the tunnel.

#### *Verifying Traffic Flow Through the DEP Tunnel*

**Purpose** Verify traffic flow across the newly-created DEP tunnel.

**Action** Run the following command on Router 2:

```
user@router2> show services ipsec-vpn ipsec statistics
PIC: ms-1/0/0, Service set: ipsec_ss_ms_5_2_01

ESP Statistics:
  Encrypted bytes:      153328
  Decrypted bytes:     131424
  Encrypted packets:    2738
  Decrypted packets:    2738
AH Statistics:
  Input bytes:          0
  Output bytes:         0
  Input packets:        0
  Output packets:       0
Errors:
  AH authentication failures: 0
  ESP authentication failures: 0
  ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
  Rule lookup failures: 0, No SA errors: 0
  Flow errors: 0, Misc errors: 0
```

### Verifying IPsec Security Associations for the Service Set

**Purpose** Verify that the security associations configured for the service set are functioning correctly.

**Action** Run the following command on Router 2:

```
user@router2> show services ipsec-vpn ipsec security-associations ipsec_ss_ms_5_2_01
Service set: ipsec_ss_ms_5_2_01, IKE Routing-instance: default
```

```
Rule: vpn_rule_ms_5_2_01, Term: term11, Tunnel index: 1
Local gateway: 10.0.1.2., Remote gateway: 10.0.1.1
IPSec inside interface: ms-1/0/0.1, Tunnel MTU: 1500
Direction SPI      AUX-SPI  Mode      Type      Protocol
inbound  1612447024  0         tunnel    dynamic   ESP
outbound 1824720964  0         tunnel    dynamic   ESP
```

### Example: NAPT Configuration for the MS-MPC

This example shows how to configure network address translation with port translation (NAPT) on an MX series router using a MultiServices Modular Port Concentrator (MS-MPC) as a services interface card.

- [Requirements on page 113](#)
- [Overview on page 113](#)
- [Configuration on page 113](#)

#### Requirements

This example uses the following hardware and software components:

- MX-series router
- MultiServices Modular Port Concentrator (MS-MPC)
- Junos OS Release 13.2R1 or higher

#### Overview

A service provider has chosen an MS-MPC as a platform to provide NAT services to accommodate new subscribers.

#### Configuration

To configure NAPT<sup>44</sup> using the MS-MPC as a services interface card, perform these tasks:

- [Configuring Interfaces on page 114](#)
- [Configure an Application Set of Acceptable ALG traffic on page 115](#)
- [Configuring a Stateful Firewall Rule on page 115](#)
- [Configuring NAT Pool and Rule on page 116](#)
- [Configuring the Service Set on page 117](#)

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```

set interfaces ge-0/2/0 unit 0 family inet address 10.255.248.2/24
set interfaces xe-1/1/0 unit 0 family inet address 10.255.247.2/24
set interfaces xe-1/1/0 unit 0 family inet service input service-set sset1
set interfaces xe-1/1/0 unit 0 family inet service output service-set sset1
set interfaces ms-3/0/0 unit 0 family inet
set applications application-set accept-algs application junos-http
set applications application-set accept-algs application junos-ftp
set applications application-set accept-algs application junos-tftp
set applications application-set accept-algs application junos-telnet
set applications application-set accept-algs application junos-sip
set applications application-set accept-algs application junos-rtcp
set services stateful-firewall rule sf-rule1 match-direction input-output
set services stateful-firewall rule sf-rule1 term sf-term1 from source-address
10.255.247.0/24
set services stateful-firewall rule sf-rule1 term sf-term1 from application-sets accept-algs
set services stateful-firewall rule sf-rule1 term sf-term1 then accept
set services nat pool napt-pool address 1.1.1.0/24
set services nat pool napt-pool port automatic
* nat rule for napt
set services nat rule nat-rule1 match-direction input
set services nat rule nat-rule1 term nat-term1 from source-address 10.255.247.0/24
set services nat rule nat-rule1 term nat-term1 from application-sets accept-algs
set services nat rule nat-rule1 term nat-term1 then translated source-pool napt-pool
set services nat rule nat-rule1 term nat-term1 then translated translation-type napt-44
* nat rule for basic nat
set services service-set sset1 stateful-firewall-rules sf-rule1
set services service-set sset1 nat-rules nat-rule1
set services service-set sset1 interface-service service-interface ms-3/0/0

```

### *Configuring Interfaces*

**Step-by-Step Procedure** Configure the interfaces required for NAT processing. You will need the following interfaces:

- A customer-facing interface that handles traffic from and to the customer.
- An internet-facing interface.
- A services interface that provides NAT and stateful firewall services to the customer-facing interface

1. Configure the interface for the customer-facing interface.

```

user@host# edit
[edit ]
user@host# set interfaces xe-1/1/0 unit 0 family inet address 10.255.247.2/24
user@host# set interfaces xe-1/1/0 unit 0 family inet service input service-set sset1
user@host# set interfaces xe-1/1/0 unit 0 family inet service output service-set sset1

```

2. Configure the interface for the Internet-facing interface.

```

[edit ]

```

```
set interfaces ge-0/2/0 unit 0 family inet address 10.255.248.2/24
```

3. Configure the interface for the service set that will connect services to the customer-facing interface. In our example, the interface resides on an MS-MPC.

```
[edit ]
```

```
user@host# set interfaces ms-3/0/0 unit 0 family inet
```

### *Configure an Application Set of Acceptable ALG traffic*

#### **Step-by-Step Procedure**

Identify the acceptable ALGs for incoming traffic.

1. Specify an application set that contains acceptable incoming ALG traffic.

```
user@host# set applications application-set accept-algs application junos-http
user@host# set applications application-set accept-algs application junos-ftp
user@host# set applications application-set accept-algs application junos-tftp
user@host# set applications application-set accept-algs application junos-telnet
user@host# set applications application-set accept-algs application junos-sip
user@host# set applications application-set accept-algs application junos-rtcp
```

#### **Results**

```
user@host#edit services applications application-set accept-algs
user@host#show
application junos-http;
application junos-ftp;
application junos-tftp;
application junos-telnet;
application junos-sip;
application junos-
```

### *Configuring a Stateful Firewall Rule*

#### **Step-by-Step Procedure**

Configure a stateful firewall rule that will accept all incoming traffic.

1. Specify firewall matching for all input and output

```
user@host# set services stateful-firewall rule sf-rule1 match-direction input-output
```

2. Identify source-address and acceptable ALG traffic from the customer-facing interface.

```
user@host# set services stateful-firewall rule sf-rule1 term sf-term1 from
source-address 10.255.247.0/24
user@host# set services stateful-firewall rule sf-rule1 term sf-term1 from
application-sets accept-algs
user@host# set services stateful-firewall rule sf-rule1 term sf-term1 then accept
```

**Results**

```
user@host# edit services stateful-firewall
user@host# show
rule sf-rule1 {
  match-direction input-output;
  term sf-term1 {
    from {
      source-address {
        10.255.247.0/24;
      }
      application-sets accept-algs;
    }
    then {
      accept;
    }
  }
}
```

### *Configuring NAT Pool and Rule*

**Step-by-Step Procedure** Configure a NAT pool and rule for address translation with automatic port assignment.

1. Configure the NAT pool with automatic port assignment.

```
user@host# set services nat pool napt-pool address 1.1.1.0/24
user@host# set services nat pool napt-pool port automatic
```

2. Configure a NAT rule that applies translation type **napt-44** using the defined NAT pool.

```
user@host# set services nat rule nat-rule1 term nat-term1 from application-sets
accept-algs
user@host# set services nat rule nat-rule1 term nat-term1 then translated source-pool
napt-pool
user@host# set services nat rule nat-rule1 term nat-term1 then translated
translation-type napt-44
```

**Results**

```

user@host#edit services nat
user@host#show

pool napt-pool {
    address 1.1.1.0/24;
    port {
        automatic;
    }
}
rule nat-rule1 {
    match-direction input;
    term nat-term1 {
        from {
            source-address {
                10.255.247.0/24;
            }
            application-sets accept-algs;
        }
        then {
            translated {
                source-pool napt-pool;
                translation-type {
                    napt-44;
                }
            }
        }
    }
}

```

### *Configuring the Service Set*

**Step-by-Step Procedure** Configure an interface type service set.

1. Specify the NAT and stateful firewall rules that apply to customer traffic.
 

```

user@host set services service-set sset1 stateful-firewall-rules sf-rule1
user@host set services service-set sset1 nat-rules bat-rule1

```
2. Specify the services interface that applies the rules to customer traffic.
 

```

set services service-set sset1 interface-service service-interface ms-3/0/0

```

**Results**

```

user@host# edit services service-set sset1
user@host# show
set services service-set sset1 stateful-firewall-rules sf-rule1
set services service-set sset1 nat-rules nat-rule1
set services service-set sset1 interface-service service-interface ms-3/0/0

```

## Examples: Services Interfaces Configuration

This section includes the following examples:

- [Example: Service Interfaces Configuration on page 118](#)
- [Example: Virtual Routing and Forwarding \(VRF\) and Service Configuration on page 121](#)

- [Example: Dynamic Source NAT as a Next-Hop Service on page 122](#)
- [Example: BOOTP and Broadcast Addresses on page 123](#)

## Example: Service Interfaces Configuration

The following configuration includes all the items necessary to configure services on an interface. For examples showing individual service configurations, see the chapters that describe each service in detail.

```
[edit]
interfaces {
  fe-0/1/0 {
    unit 0 {
      family inet {
        service {
          input {
            service-set Firewall-Set;
          }
          output {
            service-set Firewall-Set;
          }
        }
        address 10.1.3.2/24;
      }
    }
  }
  fe-0/1/1 {
    unit 0 {
      family inet {
        filter {
          input Sample;
        }
        address 172.16.1.2/24;
      }
    }
  }
  sp-1/0/0 {
    unit 0 {
      family inet {
        address 172.16.1.3/24 {
        }
      }
    }
  }
}
forwarding-options {
  sampling {
    input {
      family inet {
        rate 1;
      }
    }
    output {
      cflowd 10.1.3.1 {
        port 2055;
      }
    }
  }
}
```

```
        version 5;
    }
    flow-inactive-timeout 15;
    flow-active-timeout 60;
    interface sp-1/0/0 {
        engine-id 1;
        engine-type 136;
        source-address 10.1.3.2;
    }
}
}
}
}
firewall {
    filter Sample {
        term Sample {
            then {
                count Sample;
                sample;
                accept;
            }
        }
    }
}
}
services {
    stateful-firewall {
        rule Rule1 {
            match-direction input;
            term 1 {
                from {
                    application-sets Applications;
                }
                then {
                    accept;
                }
            }
            term accept {
                then {
                    accept;
                }
            }
        }
    }
    rule Rule2 {
        match-direction output;
        term Local {
            from {
                source-address {
                    10.1.3.2/32;
                }
            }
            then {
                accept;
            }
        }
    }
}
}
ids {
```

```
rule Attacks {
  match-direction output;
  term Match {
    from {
      application-sets Applications;
    }
    then {
      logging {
        syslog;
      }
    }
  }
}

nat {
  pool public {
    address-range low 172.16.2.1 high 172.16.2.32;
    port automatic;
  }
  rule Private-Public {
    match-direction input;
    term Translate {
      then {
        translated {
          source-pool public;
          translation-type source napt-44;
        }
      }
    }
  }
}

service-set Firewall-Set {
  stateful-firewall-rules Rule1;
  stateful-firewall-rules Rule2;
  nat-rules Private-Public;
  ids-rules Attacks;
  interface-service {
    service-interface sp-1/0/0;
  }
}

applications {
  application ICMP {
    application-protocol icmp;
  }
  application FTP {
    application-protocol ftp;
    destination-port ftp;
  }
  application-set Applications {
    application ICMP;
    application FTP;
  }
}
```

## Example: Virtual Routing and Forwarding (VRF) and Service Configuration

The following example combines virtual routing and forwarding (VRF) and services configuration:

```
[edit policy-options]
policy-statement test-policy {
  term t1 {
    then reject;
  }
}
[edit routing-instances]
test {
  interface ge-0/2/0.0;
  interface sp-1/3/0.20;
  instance-type vrf;
  route-distinguisher 10.58.255.1:37;
  vrf-import test-policy;
  vrf-export test-policy;
  routing-options {
    static {
      route 0.0.0.0/0 next-table inet.0;
    }
  }
}
[edit interfaces]
ge-0/2/0 {
  unit 0 {
    family inet {
      service {
        input service-set nat-me;
        output service-set nat-me;
      }
    }
  }
}
sp-1/3/0 {
  unit 0 {
    family inet;
  }
  unit 20 {
    family inet;
    service-domain inside;
  }
  unit 21 {
    family inet;
    service-domain outside;
  }
}
[edit services]
stateful-firewall {
  rule allow-any-input {
    match-direction input;
    term t1 {
      then accept;
    }
  }
}
```

```
    }  
  }  
  nat {  
    pool hide-pool {  
      address 10.58.16.100;  
      port automatic;  
    }  
    rule hide-all-input {  
      match-direction input;  
      term t1 {  
        then {  
          translated {  
            source-pool hide-pool;  
            translation-type source napt-44;  
          }  
        }  
      }  
    }  
  }  
}  
service-set nat-me {  
  stateful-firewall-rules allow-any-input;  
  nat-rules hide-all-input;  
  interface-service {  
    service-interface sp-1/3/0.20;  
  }  
}
```

### Example: Dynamic Source NAT as a Next-Hop Service

The following example shows dynamic-source NAT applied as a next-hop service:

```
[edit interfaces]  
ge-0/2/0 {  
  unit 0 {  
    family mpls;  
  }  
}  
sp-1/3/0 {  
  unit 0 {  
    family inet;  
  }  
  unit 20 {  
    family inet;  
  }  
  unit 32 {  
    family inet;  
  }  
}  
[edit routing-instances]  
protected-domain {  
  interface ge-0/2/0.0;  
  interface sp-1/3/0.20;  
  instance-type vrf;  
  route-distinguisher 10.58.255.17:37;  
  vrf-import protected-domain-policy;  
}
```

```

vrf-export protected-domain-policy;
routing-options {
  static {
    route 0.0.0.0/0 next-hop sp-1/3/0.20;
  }
}
[edit policy-options]
policy-statement protected-domain-policy {
  term t1 {
    then reject;
  }
}
[edit services]
stateful-firewall {
  rule allow-all {
    match-direction input;
    term t1 {
      then {
        accept;
      }
    }
  }
}
nat {
  pool my-pool {
    address 10.58.16.100;
    port automatic;
  }
  rule hide-all {
    match-direction input;
    term t1 {
      then {
        translated {
          source-pool my-pool;
          translation-type napt-44;
        }
      }
    }
  }
}
service-set null-sfw-with-nat {
  stateful-firewall-rules allow-all;
  nat-rules hide-all;
  next-hop-service {
    inside-service-interface sp-1/3/0.20;
    outside-service-interface sp-1/3/0.32;
  }
}

```

### Example: BOOTP and Broadcast Addresses

The following example supports Bootstrap Protocol (BOOTP) and broadcast addresses:

```

[edit applications]
application bootp {

```

```
    application-protocol bootp;
    protocol udp;
    destination-port 67;
  }
[edit services]
stateful-firewall bootp-support {
  rule bootp-allow {
    direction input;
    term bootp-allow {
      from {
        destination-address {
          any-unicast;
          255.255.255.255;
        }
        application bootp;
      }
      then {
        accept;
      }
    }
  }
}
```

## CHAPTER 4

# Applications Configuration Guidelines

You can define application protocols for the stateful firewall and Network Address Translation (NAT) services to use in match condition rules. An application protocol, or application layer gateway (ALG), defines application parameters using information from network Layer 3 and above. Examples of such applications are FTP and H.323.

To configure applications that are used with services, include the following statements at the **[edit applications]** hierarchy level:

```
[edit applications]
application application-name {
  application-protocol protocol-name;
  destination-port port-number;
  icmp-code value;
  icmp-type value;
  inactivity-timeout value;
  learn-sip-register;
  protocol type;
  rpc-program-number number;
  sip-call-hold-timeout seconds;
  snmp-command command;
  source-port port-number;
  ttl-threshold value;
  uuid hex-value;
}
application-set application-set-name {
  application application-name;
}
```

This chapter includes the following sections:

- [ALG Descriptions on page 126](#)
- [Configuring Application Protocol Properties on page 146](#)
- [Configuring Application Sets on page 163](#)
- [Verifying the Output of ALG Sessions on page 164](#)
- [Junos Default Groups on page 170](#)
- [Examples: Configuring Application Protocols on page 177](#)

## ALG Descriptions

This topic describes the Application Layer Gateways (ALGs) supported by the Junos OS. ALG support includes managing pinholes and parent-child relationships for the supported all ALGs. This topic includes the following section:

- [Supported ALGs on page 126](#)
- [ALG Support Details on page 127](#)
- [Juniper Networks Defaults on page 136](#)

## Supported ALGs

Table 16 on page 126 lists ALGs supported by the Junos OS.

**Table 16: ALGs Supported by the Junos OS**

ALGs Supported	v4 - v4	v4 - v6	v6 - v6	DS-Lite
Basic TCP ALG	Yes	Yes	Yes	Yes
Basic UPD ALG	Yes	Yes	Yes	Yes
BOOTP	Yes	No	No	No
DCE RPC Services	Yes	No	No	No
DNS	Yes	Yes	No	No
FTP	Yes	No	No	Yes
H323	Yes	No	No	No
ICMP	Yes	Yes	Yes	Yes
IIOIP	Yes	No	No	No
IP	Yes	No	No	No
NETBIOS	Yes	No	No	No
NETSHOW	Yes	No	No	No
PPTP	Yes	No	No	Yes
REALAUDIO	Yes	No	No	No
Sun RPC and RPC Port Map Services	Yes	No	No	No
RTSP	Yes	No	No	Yes

Table 16: ALGs Supported by the Junos OS (*continued*)

ALGs Supported	v4 - v4	v4 - v6	v6 - v6	DS-Lite
SIP	Yes	No	No	No
SNMP	Yes	No	No	No
SQLNET	Yes	No	No	No
TFTP	Yes	No	No	Yes
Traceroute	Yes	Yes	No	Yes
Unix Remote Shell Service	Yes	No	No	No
WINFrame	Yes	No	No	No

## ALG Support Details

This section includes details about the ALGs. It includes the following:

- [Basic TCP ALG on page 128](#)
- [Basic UDP ALG on page 128](#)
- [BOOTP on page 129](#)
- [DCE RPC Services on page 129](#)
- [DNS on page 129](#)
- [FTP on page 129](#)
- [H323 on page 130](#)
- [ICMP on page 130](#)
- [IIOP on page 130](#)
- [IP on page 131](#)
- [NetBIOS on page 131](#)
- [NetShow on page 131](#)
- [ONC RPC Services on page 131](#)
- [PPTP on page 131](#)
- [RealAudio on page 132](#)
- [Sun RPC and RPC Portmap Services on page 132](#)
- [RTSP on page 134](#)
- [SIP on page 134](#)
- [SNMP on page 135](#)
- [SQLNet on page 135](#)
- [TFTP on page 135](#)

- [Traceroute on page 135](#)
- [UNIX Remote-Shell Services on page 136](#)
- [Winframe on page 136](#)

### Basic TCP ALG

---

This ALG performs basic sanity checking on TCP packets. If it finds errors, it generates the following anomaly events and system log messages:

- TCP source or destination port zero
- TCP header length check failed
- TCP sequence number zero and no flags are set
- TCP sequence number zero and FIN/PSH/RST flags are set
- TCP FIN/RST or SYN(URG|FIN|RST) flags are set

The TCP ALG performs the following steps:

1. When the router receives a SYN packet, the ALG creates TCP forward and reverse flows and groups them in a *conversation*. It tracks the TCP three-way handshake.
2. The SYN-defense mechanism tracks the TCP connection establishment state. It expects the TCP session to be established within a small time interval (currently 4 seconds). If the TCP three-way handshake is not established in that period, the session is terminated.
3. A keepalive mechanism detects TCP sessions with nonresponsive endpoints.
4. ICMP errors are allowed only if there is a flow that matches the selector information specified in the ICMP data.

### Basic UDP ALG

---

This ALG performs basic sanity checking on UDP headers. If it finds errors, it generates the following anomaly events and system log messages:

- UDP source or destination port 0
- UDP header length check failed

The UDP ALG performs the following steps:

1. When it receives the first packet, the ALG creates bidirectional flows to accept forward and reverse UDP session traffic.
2. If the session is idle for more than the maximum allowed idle time (the default is 30 seconds), the flows are deleted.
3. ICMP errors are allowed only if there is a flow that matches the selector information specified in the ICMP data.

## BOOTP

---

The Bootstrap Protocol (BOOTP) client retrieves its networking information from a server across the network. It sends out a general broadcast message to request the information, which is returned by the BOOTP server. For the protocol specification, see <ftp://ftp.isi.edu/in-notes/rfc951.txt>.

Stateful firewall support requires that you configure the BOOTP ALG on UDP server port 67 and client port 68. If the client sends a broadcast message, you should configure the broadcast address in the **from** statement of the service rule. Network Address Translation (NAT) is not performed on the BOOTP traffic, even if the NAT rule matches the traffic. If the BOOTP relay feature is activated on the router, the remote BOOTP server is assumed to assign addresses for clients masked by NAT translation.

## DCE RPC Services

---

Distributed Computing Environment (DCE) Remote Procedure Call (RPC) services are mainly used by Microsoft applications. The ALG uses well-known TCP port 135 for port mapping services, and uses the universal unique identifier (UUID) instead of the program number to identify protocols. The main application-based DCE RPC is the Microsoft Exchange Protocol.

Support for stateful firewall and NAT services requires that you configure the DCE RPC portmap ALG on TCP port 135. The DCE RPC ALG uses the TCP protocol with application-specific UUIDs.

## DNS

---

The Domain Name Service (DNS) ALG handles data associated with locating and translating domain names into IP addresses. The ALG typically runs on port 53. The ALG monitors DNS query and reply packets and supports only UDP traffic. The ALG does not support payload translations. The DNS ALG will only close the session when a reply is received or an idle timeout is reached.

## FTP

---

FTP is the File Transfer Protocol, specified in RFC 959. In addition to the main control connection, data connections are also made for any data transfer between the client and the server; and the host, port, and direction are negotiated through the control channel.

For non-passive-mode FTP, the Junos OS stateful firewall service scans the client-to-server application data for the PORT command, which provides the IP address and port number to which the server connects. For passive-mode FTP, the Junos OS stateful firewall service scans the client-to-server application data for the PASV command and then scans the server-to-client responses for the 227 response, which contains the IP address and port number to which the client connects.

There is an additional complication: FTP represents these addresses and port numbers in ASCII. As a result, when addresses and ports are rewritten, the TCP sequence number might be changed, and thereafter the NAT service needs to maintain this delta in SEQ and ACK numbers by performing sequence NAT on all subsequent packets.

Support for stateful firewall and NAT services requires that you configure the FTP ALG on TCP port 21 to enable the FTP control protocol. The ALG performs the following tasks:

- Automatically allocates data ports and firewall permissions for dynamic data connection
- Creates flows for the dynamically negotiated data connection
- Monitors the control connection in both active and passive modes
- Rewrites the control packets with the appropriate NAT address and port information

---

### H323

H323 is a suite of ITU protocols for audio and video conferencing and collaboration applications. H323 consists of H.225 call signaling protocols and H.245 control protocol for media communication. During H.225 negotiation, the endpoints create a call by exchanging call signaling messages on the control channel and negotiate a new control channel for H.245. A new control connection is created for H.245 messages. Messages are exchanged on the H.245 control channel to open media channels.

Stateful firewall monitors the H.225 control channel to open the H.245 control channel. After the H.245 channel is created, stateful firewall also monitors this channel for media channel information and allows the media traffic through the firewall.

H323 ALG supports static destination, static and dynamic source NAT by rewriting the appropriate addresses and ports in the H.225 and H.245 messages.

---

### ICMP

The Internet Control Message Protocol (ICMP) is defined in RFC 792. The Junos OS stateful firewall service allows ICMP messages to be filtered by specific type or specific type code value. ICMP error packets that lack a specifically configured type and code are matched against any existing flow in the opposite direction to check for the legitimacy of the error packet. ICMP error packets that pass the filter matching are subject to NAT translation.

The ICMP ALG always tracks ping traffic statefully using the ICMP sequence number. Each echo reply is forwarded only if there is an echo request with the corresponding sequence number. For any ping flow, only 20 echo requests can be forwarded without receiving an echo reply. When you configure dynamic NAT, the PING packet identifier is translated to allow additional hosts in the NAT pool to use the same identifier.

Support for stateful firewall and NAT services requires that you configure the ICMP ALG if the protocol is needed. You can configure the ICMP type and code for additional filtering.

---

### IIOP

The Oracle Application Server NameServer Internet Inter-ORB Protocol (IIOP). This ALG is used in Common Object Request Broker Architecture (CORBA) based on distributed computing. Even though CORBA and IIOP are Object Management Group (OMG) standards, there is no fixed port assigned for IIOP. Each vendor implementing CORBA chooses a port. Java Virtual machine uses port 1975 by default, while ORBIX uses port 3075 as a default.

Stateful firewall and NAT require ALG IOP be configured for TCP port 1975 for Java VM IOP, and 3075 for CORBA applications ORBIX, a CORBA framework from Iona Technologies.

## IP

---

The IP ALG is used to create uni-directional flows only. In case of TCP traffic, it does not check the 3-way handshake process. This ALG is useful in case of stateful firewall only service sets, where it allows traffic to flow uni-directionally only. When configuring in conjunction with **match-direction input-output** it allows the return traffic to flow through the stateful firewall as well. Typical scenarios are static NAT, destination NAT or scenarios where traffic is expected to traverse the stateful firewall in the presence of asymmetric routing. The Junos IP ALG is not intended for use with NAT, which will cause matching traffic to be discarded through the creation of a drop flow.

## NetBIOS

---

A NetBIOS ALG translates NetBIOS IP addresses and port numbers when NAT is used.

NetBIOS supports the TCP and UDP transport protocols. Support for stateful firewall and NAT services requires that you configure the NetBIOS ALG on UDP port 138 and TCP port 139.

## NetShow

---

The Microsoft protocol ms-streaming is used by NetShow, the Microsoft media server. This protocol supports several transport protocols: TCP, UDP, and HTTP. The client starts a TCP connection on port 1755 and sends the PORT command to the server. The server then starts UDP on that port to the client. Support for stateful firewall and NAT services requires that you configure the NetShow ALG on UDP port 1755.

## ONC RPC Services

---

Open Networks Computing (ONC) RPC services function similarly to DCE RCP services. However, the ONC RPC ALG uses TCP/UDP port 111 for port mapping services, and uses the program number to identify protocols rather than the UUID.

Support for stateful firewall and NAT services requires that you configure the ONC RPC portmap ALG on TCP port 111. The ONC RPC ALG uses the TCP protocol with application-specific program numbers.

## PPTP

---

The Point-to-Point Tunneling Protocol (PPTP) ALG is a TCP-based ALG. PPTP allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP defines a client-server architecture, a PPTP Network Server, and a PPTP Access Concentrator. The PPTP ALG requires a control connection and a data tunnel. The control connection uses TCP to establish and disconnect PPP sessions, and runs on port 1723. The data tunnel carries PPP traffic in generic routing encapsulated (GRE) packets that are carried over IP.

## RealAudio

Real Networks PNA protocol RealVideo is not a separate service. It is part of the RealPlayer and most likely uses another channel for video. The RealPlayer versions G2, 7, and 8 use PNA and RTSP. For this version to work, the ALG must allow both PNA(7070) and RTSP(554). For the media, the server selects from a range of UDP ports(6970 through 7170), or TCP port 7071, or HTTP. The client can be configured to use a particular port. The RealPlayer versions 4.0 and 5.0 use control channel 7070 media UDP ports 6970 through 7170, or TCP port 7071, or HTTP. RealAudio player version 3.0 uses control channel 7070 media, UDP ports 6770-7170, or TCP port 7071.

Real products use the ports and ranges of ports shown in [Table 17 on page 132](#).

**Table 17: RealAudio Product Port Usage**

Real Product	Port Usage
4.0 and 5.0 Servers/Players	Control channel (bidirectional) on TCP port 7070. Data channel from server to player on TCP port 7070 or UDP port 6970-7170.
4.0 and 5.0 Servers/Encoders	Control channel (bidirectional) on TCP port 7070. Data channel from encoder or server on TCP port 7070.
G2 Servers/Players	Control channel (bidirectional) on TCP port 80, 554, 7070, or 8080. Data channel from server to player on TCP port 80, 554, 7070, 8080 or UDP port 6970-32,000.
G2 Server/3.1, and 5.x Encoders	Control channel (bidirectional) on TCP port 7070. Data channel from encoder to server on TCP port 7070.
G2 Server/G2 Producer	Control channel (bidirectional) on TCP port 4040. Data channel from encoder to server on TCP port 4040 and UDP port 6970-32,000.
2 Server/G2 Producer (TCP ONLY)	Control channel (bidirectional) on TCP port 4040 Data channel from encoder to server on TCP port 4040. Note: TCP-ONLY option available in version 6.1 or above.



**NOTE:** RealAudio was the original protocol by RealPlayers. Newer versions of RealPlayer use RTSP. Stateful firewall and NAT require ALG RealAudio to be programmed on TCP port 7070.

## Sun RPC and RPC Portmap Services

The Remote Procedure Call (RPC) ALG uses well-known ports TCP 111 and UDP 111 for port mapping, which dynamically assigns and opens ports for RPC services. The RPC Portmap ALG keeps track of port requests and dynamically opens the firewall for these requested ports. The RPC ALG can further restrict the RPC protocol by specifying allowed program numbers.

The ALG includes the RPC services listed in [Table 18 on page 133](#).

Table 18: Supported RPC Services

Name	Description	Comments
<b>rpc.mountd</b>	Network File Server (NFS) mount daemon; for details, see the UNIX man page for <b>rpc.mountd(8)</b> .	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050).
<b>rpc.nfsprog</b>	Used as part of NFS. For details, see RFC 1094. See also RFC1813 for NFS v3.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050).
<b>rpc.nisplus</b>	Network Information Service Plus (NIS+), designed to replace NIS; it is a default naming service for Sun Solaris and is not related to the old NIS. No protocol information is available.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050).
<b>rpc.nlockmgr</b>	Network lock manager.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, <b>rpc.nlockmgr</b> service can be allowed or blocked based on RPC program 100021.
<b>rpc.pcnfsd</b>	Kernel statistics server. For details, see the UNIX man pages for <b>rstatd</b> and <b>rpc.rstatd</b> .	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, <b>rpc.rstat</b> service can be allowed or blocked based on RPC program 150001.
<b>rpc.rwall</b>	Used to write a message to users; for details, see the UNIX man page for <b>rpc.rwalld</b> .	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, <b>rpc.rwall</b> service can be allowed or blocked based on RPC program 150008.
<b>rpc.ybind</b>	NIS binding process. For details, see the UNIX man page for <b>ybind</b> .	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, <b>rpc.ybind</b> service can be allowed or blocked based on RPC program 100007.
<b>rpc.yppasswd</b>	NIS password server. For details, see the UNIX man page for <b>yppasswd</b> .	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, <b>rpc.yppasswd</b> service can be allowed or blocked based on RPC program 100009.
<b>rpc.ypserv</b>	NIS server. For details, see the UNIX man page for <b>ypserv</b> .	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, <b>rpc.ypserv</b> service can be allowed or blocked based on RPC program 100004.
<b>rpc.yupdated</b>	Network updating tool.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, <b>rpc.yupdated</b> service can be allowed or blocked based on RPC program 100028.
<b>rpc.ypxfrd</b>	NIS map transfer server. For details, see the UNIX man page for <b>rpc.ypxfrd</b> .	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, <b>rpc.ypxfrd</b> service can be allowed or blocked based on RPC program 100069.

Support for stateful firewall and NAT services that use port mapping requires that you configure the RPC portmap ALG on TCP/UDP destination port 111 and the RPC ALG for both TCP and UDP. You can specify one or more **rpc-program-number** values to further restrict allowed RPC protocols.

## RTSP

---

The Real-Time Streaming Protocol (RTSP) controls the delivery of data with real-time properties such as audio and video. The streams controlled by RTSP can use RTP, but it is not required. Media can be transmitted on the same RTSP control stream. This is an HTTP-like text-based protocol, but client and server maintain session information. A session is established using the SETUP message and terminated using the TEARDOWN message. The transport (the media protocol, address, and port numbers) is negotiated in the setup and the setup-response.

Support for stateful firewall and NAT services requires that you configure the RTSP ALG for TCP port 554.

The ALG monitors the control connection, opens flows dynamically for media (RTP/RTSP) streams, and performs NAT address and port rewrites.

## SIP

---

The Session Initiation Protocol (SIP) is an application layer protocol that can establish, maintain, and terminate media sessions. It is a widely used voice over IP (VoIP) signaling protocol. The SIP ALG monitors SIP traffic and dynamically creates and manages pinholes on the signaling and media paths. The ALG only allows packets with the correct permissions. The SIP ALG also performs the following functions:

- Manages parent-child session relationships.
- Enforces security policies.
- Manages pinholes for VoIP traffic.

The SIP ALG supports the following features:

- Stateful firewall
- Static source NAT
- Dynamic address only source NAT
- Network Address Port Translation (NAPT)



**NOTE:** SIP sessions are limited to 12 hours (720 minutes) for NAT processing on the MS-MIC and MS-MPC interface cards. There is no time limit for SIP sessions on the MS-DPC.

---

## SNMP

---

SNMP is a communication protocol for managing TCP/IP networks, including both individual network devices and aggregated devices. The protocol is defined by RFC 1157. SNMP runs on top of UDP.

The Junos OS stateful firewall service implements the SNMP ALG to inspect the SNMP type. SNMP does not enforce stateful flow. Each SNMP type needs to be specifically enabled. Full SNMP support of stateful firewall services requires that you configure the SNMP ALG on UDP port 161. This enables the SNMP **get** and **get-next** commands, as well as their response traffic in the reverse direction: UDP port 161 enables the SNMP **get-response** command. If SNMP traps are permitted, you can configure them on UDP port 162, enabling the SNMP **trap** command.

## SQLNet

---

The SQLNet protocol is used by Oracle SQL servers to execute SQL commands from clients, including load balancing and application-specific services.

Support of stateful firewall and NAT services requires that you configure the SQLNet ALG for TCP port 1521.

The ALG monitors the control packets, opens flows dynamically for data traffic, and performs NAT address and port rewrites.

## TFTP

---

The Trivial File Transfer Protocol (TFTP) is specified in RFC 1350. The initial TFTP requests are sent to UDP destination port 69. Additional flows can be created to **get** or **put** individual files. Support of stateful firewall and NAT services requires that you configure the TFTP ALG for UDP destination port 69.

## Traceroute

---

Traceroute is a tool for displaying the route that packets take to a network host. It uses the IP time-to-live (TTL) field to trigger ICMP time-exceeded messages from routers or gateways. It sends UDP datagrams to destination ports that are believed to be not in use; destination ports are numbered using the formula:  $+ n\text{hops} - 1$ . The default base port is 33434. To support traceroute through the firewall, two types of traffic must be passed through:

1. UDP probe packets (UDP destination port  $> 33000$ , IP TTL  $< 30$ )
2. ICMP response packets (ICMP type time-exceeded)

When NAT is applied, the IP address and port within the ICMP error packet also must be changed.

Support of stateful firewall and NAT services requires you to configure the Traceroute ALG for UDP destination port 33434 to 33450. In addition, you can configure the TTL threshold to prevent UDP flood attacks with large TTL values.

## UNIX Remote-Shell Services

---

Three protocols form the basis for UNIX remote-shell services:

- Exec—Remote command execution; enables a user on the client system to execute a command on the remote system. The first command from client (**rcmd**) to server (**rshd**) uses well-known TCP port 512. A second TCP connection can be opened at the request of **rcmd**. The client port number for the second connection is sent to the server as an ASCII string.
- Login—Better known as **rlogin**; uses well-known TCP port 513. For details, see RFC 1282. No special firewall processing is required.
- Shell—Remote command execution; enables a user on the client system to execute a command on the remote system. The first command from client (**rcmd**) to server (**rshd**) uses well-known TCP port 514. A second TCP connection can be opened at the request of **rcmd**. The client port number for the second connection is sent to the server as an ASCII string.

Support of stateful firewall services requires that you configure the Exec ALG on TCP port 512, the Login ALG on TCP port 513, and the Shell ALG on TCP port 514. NAT remote-shell services require that any dynamic source port assigned be within the port range 512 to 1023. If you configure a NAT pool, this port range is reserved exclusively for remote shell applications.

## Winframe

---

WinFrame application server software provides access to virtually any Windows application, across any type of network connection to any type of client.

This protocol is mainly used by Citrix Windows applications.

Stateful firewall and NAT require the ALG Winframe to be configured on TCP destination port 1494 and UDP port 1604.

## Juniper Networks Defaults

```
applications {
  #
  # File Transfer Protocol
  #
  application junos-ftp {
    application-protocol ftp;
    protocol tcp;
    destination-port 21;
  }
  #
  # Trivial File Transfer Protocol
  #
  application junos-tftp {
    application-protocol tftp;
    protocol udp;
    destination-port 69;
  }
}
```

```
#
# RPC portmapper on TCP
#
application junos-rpc-portmap-tcp {
    application-protocol rpc-portmap;
    protocol tcp;
    destination-port 111;
}
#
# RPC portmapper on UDP
#
application junos-rpc-portmap-udp {
    application-protocol rpc-portmap;
    protocol udp;
    destination-port 111;
}
#
# SNMP get
#
application junos-snmp-get {
    application-protocol snmp;
    protocol udp;
    destination-port 161;
    snmp-command get;
}
#
# SNMP get next
#
application junos-snmp-get-next {
    application-protocol snmp;
    protocol udp;
    destination-port 161;
    snmp-command get-next;
}
#
# SNMP response
#
application junos-snmp-response {
    application-protocol snmp;
    protocol udp;
    source-port 161;
    snmp-command get-response;
}
#
# SNMP trap
#
application junos-snmp-trap {
    application-protocol snmp;
    protocol udp;
    destination-port 162;
    snmp-command trap;
}
#
# remote exec
#
application junos-rexec {
```

```
    application-protocol exec;
    protocol tcp;
    destination-port 512;
}
#
# remote login
#
application junos-rlogin {
    application-protocol shell;
    protocol tcp;
    destination-port 513;
}
#
# remote shell
#
application junos-rsh {
    application-protocol shell;
    protocol tcp;
    destination-port 514;
}
#
# Real Time Streaming Protocol
#
application junos-rtsp {
    application-protocol rtsp;
    protocol tcp;
    destination-port 554;
}
#
# Citrix windows application server protocol
# windows applications remotely on windows/non-windows clients
#
# citrix needs udp 1604 to be open
#
application junos-citrix-winframe {
    application-protocol winframe;
    protocol tcp;
    destination-port 1494;
}
application junos-citrix-winframe-udp {
    protocol udp;
    destination-port 1604;
}
#
# Oracle SQL servers use this protocol to execute sql commands
# from clients, load balance, use application-specific servers, etc
#
application junos-sqlnet {
    application-protocol sqlnet;
    protocol tcp;
    destination-port 1521;
}
#
# H.323 Protocol for audio/video conferencing
#
application junos-h323 {
```

```
    application-protocol h323;
    protocol tcp;
    destination-port 1720;
}
#
# Internet Inter-ORB Protocol - used for CORBA applications
# The ORB protocol in Java virtual machines uses port 1975 as default
#
application junos-iiop-java {
    application-protocol iiop;
    protocol tcp;
    destination-port 1975;
}
#
# Internet Inter-ORB Protocol - used for CORBA applications
# ORBIX is a CORBA framework from Iona Technologies that uses port
# 3075 as default
#
application junos-iiop-orbix {
    application-protocol iiop;
    protocol tcp;
    destination-port 3075;
}
#
# Real players use this protocol for real time streaming
# This was the original protocol for real players.
# RTSP is more widely used by real players
# but they still support realaudio.
#
application junos-realaudio {
    application-protocol realaudio;
    protocol tcp;
    destination-port 7070;
}
#
# traceroute application.
#
application junos-traceroute {
    application-protocol traceroute;
    protocol udp;
    destination-port 33435-33450;
    ttl-threshold 30;
}
#
# The full range of known RPC programs using UDP
# The program numbers can be more specific to certain applications.
#
application junos-rpc-services-udp {
    application-protocol rpc;
    protocol udp;
    rpc-program-number 100000-400000;
}
#
# The full range of known RPC programs using TCP
# The program numbers can be more specific to certain applications.
#
```

```
application junos-rpc-services-tcp {
  application-protocol rpc;
  protocol tcp;
  rpc-program-number 100000-400000;
}
#
# All ICMP traffic
# This can be made to be more restrictive by specifying ICMP type
# and code.
#
application junos-icmp-all {
  application-protocol icmp;
}
#
# Protocol used by Windows media server and windows media player
#
application junos-netshow {
  application-protocol netshow;
  protocol tcp;
  destination-port 1755;
}
#
# NetBIOS - networking protocol used on
# Windows networks name service port, both UDP and TCP
#
application junos-netbios-name-udp {
  application-protocol netbios;
  protocol udp;
  destination-port 137;
}
application junos-netbios-name-tcp {
  protocol tcp;
  destination-port 137;
}
#
# NetBIOS - networking protocol used on
# Windows networks datagram service port
#
application junos-netbios-datagram {
  application-protocol netbios;
  protocol udp;
  destination-port 138;
}
#
# NetBIOS - networking protocol used on
# Windows networks session service port
#
application junos-netbios-session {
  protocol tcp;
  destination-port 139;
}
#
# DCE-RPC portmapper on TCP
#
application junos-dce-rpc-portmap {
  application-protocol dce-rpc-portmap;
```

```

    protocol tcp;
    destination-port 135;
}
#
# DCE-RPC application on TCP sample UUID
# This application requires user to specify the UUID value
#
# application junos-dcerpc {
#   application-protocol dce-rpc;
#   protocol tcp;
#
#   # UUID also needs to be defined as shown below
#   UUID 11223344 22334455 33445566 44556677;
#
# }
#
# ms-exchange needs these 3 UUIDs
#
application junos-dcerpc-endpoint-mapper-service {
    application-protocol dce-rpc;
    protocol tcp;
    uuid e1af8308-5d1f-11c9-91a4-08002b14a0fa;
}
application junos-dcerpc-msexchange-directory-rfr {
    application-protocol dce-rpc;
    protocol tcp;
    uuid 1544f5e0-613c-11d1-93df-00c04fd7bd09;
}
application junos-dcerpc-msexchange-information-store {
    application-protocol dce-rpc;
    protocol tcp;
    uuid a4f1db00-ca47-1067-b31f-00dd010662da;
}
application junos-ssh {
    protocol tcp;
    destination-port 22;
}
application junos-telnet {
    protocol tcp;
    destination-port 23;
}
application junos-smtp {
    protocol tcp;
    destination-port 25;
}
application junos-dns-udp {
    protocol udp;
    destination-port 53;
}
application junos-dns-tcp {
    protocol tcp;
    destination-port 53;
}
application junos-tacacs {
    protocol tcp;
    destination-port 49;
}

```

```
}
# TACACS Database Service
application junos-tacacs-ds {
    protocol tcp;
    destination-port 65;
}
application junos-dhcp-client {
    protocol udp;
    destination-port 68;
}
application junos-dhcp-server {
    protocol udp;
    destination-port 67;
}
application junos-bootpc {
    protocol udp;
    destination-port 68;
}
application junos-bootps {
    protocol udp;
    destination-port 67;
}
application junos-finger {
    protocol tcp;
    destination-port 79;
}
application junos-http {
    protocol tcp;
    destination-port 80;
}
application junos-https {
    protocol tcp;
    destination-port 443;
}
application junos-pop3 {
    protocol tcp;
    destination-port 110;
}
application junos-ident {
    protocol tcp;
    destination-port 113;
}
application junos-nntp {
    protocol tcp;
    destination-port 119;
}
application junos-ntp {
    protocol udp;
    destination-port 123;
}
application junos-imap {
    protocol tcp;
    destination-port 143;
}
application junos-imaps {
    protocol tcp;
```

```
        destination-port 993;
    }
    application junos-bgp {
        protocol tcp;
        destination-port 179;
    }
    application junos-ldap {
        protocol tcp;
        destination-port 389;
    }
    application junos-snpp {
        protocol tcp;
        destination-port 444;
    }
    application junos-biff {
        protocol udp;
        destination-port 512;
    }
    # UNIX who
    application junos-who {
        protocol udp;
        destination-port 513;
    }
    application junos-syslog {
        protocol udp;
        destination-port 514;
    }
    # line printer daemon, printer, spooler
    application junos-printer {
        protocol tcp;
        destination-port 515;
    }
    # UNIX talk
    application junos-talk-tcp {
        protocol tcp;
        destination-port 517;
    }
    application junos-talk-udp {
        protocol udp;
        destination-port 517;
    }
    application junos-ntalk {
        protocol udp;
        destination-port 518;
    }
    application junos-rip {
        protocol udp;
        destination-port 520;
    }
    # INA sanctioned RADIUS port numbers
    application junos-radius {
        protocol udp;
        destination-port 1812;
    }
    application junos-radacct {
        protocol udp;
```

```
        destination-port 1813;
    }
    application junos-nfsd-tcp {
        protocol tcp;
        destination-port 2049;
    }
    application junos-nfsd-udp {
        protocol udp;
        destination-port 2049;
    }
    application junos-cvspserver {
        protocol tcp;
        destination-port 2401;
    }
    #
    # Label Distribution Protocol
    #
    application junos-ldp-tcp {
        protocol tcp;
        destination-port 646;
    }
    application junos-ldp-udp {
        protocol udp;
        destination-port 646;
    }
    #
    # JUNOScript and JUNOScope management
    #
    application junos-xnm-ssl {
        protocol tcp;
        destination-port 3220;
    }
    application junos-xnm-clear-text {
        protocol tcp;
        destination-port 3221;
    }
    #
    # IPsec tunnel
    #
    application junos-ipsec-esp {
        protocol esp;
    }
    application junos-ike {
        protocol udp;
        destination-port 500;
    }
    #
    # 'junos-algs-outbound' defines a set of all applications
    # requiring an ALG. Useful for defining rule to the the public
    # internet allowing private network users to use all JUNOS OS
    # supported ALGs initiated from the private network.
    #
    # NOTE: the contents of this set might grow in future JUNOS OS versions.
    #
    application-set junos-algs-outbound {
        application junos-ftp;
```

```

application junos-tftp;
application junos-rpc-portmap-tcp;
application junos-rpc-portmap-udp;
application junos-snmp-get;
application junos-snmp-get-next;
application junos-snmp-response;
application junos-snmp-trap;
application junos-rexec;
application junos-rlogin;
application junos-rsh;
application junos-rtsp;
application junos-citrix-winfile;
application junos-citrix-winfile-udp;
application junos-sqlnet;
application junos-h323;
application junos-iiop-java;
application junos-iiop-orbix;
application junos-realaudio;
application junos-traceroute;
application junos-rpc-services-udp;
application junos-rpc-services-tcp;
application junos-icmp-all;
application junos-netshow;
application junos-netbios-name-udp;
application junos-netbios-datagram;
application junos-dcerpc-endpoint-mapper-service;
application junos-dcerpc-msexchange-directory-rfr;
application junos-dcerpc-msexchange-information-store;
}
#
# 'junos-management-inbound' represents the group of applications
# that might need access the router from public network for
# for management purposes.
#
# Set is intended for a UI to display management choices.
#
# NOTE: It is not recommended the user to use the entire set
# directly in a firewall rule and open up firewall to all
# of these applications. Also, the user should always
# specify the source and destination prefixes when using
# each application.
#
# NOTE: the contents of this set may grow in future JUNOS versions.
#
application-set junos-management-inbound {
    application junos-snmp-get;
    application junos-snmp-get-next;
    application junos-snmp-response;
    application junos-snmp-trap;
    application junos-ssh;
    application junos-telnet;
    application junos-http;
    application junos-https;
    application junos-xnm-ssl;
    application junos-xnm-clear-text;
}

```

```
#
# 'junos-routing-inbound' represents routing protocols that might
# need to access the router from public network.
#
# Set is intended for a UI to display routing involvement choices.
#
# NOTE: It is not recommended the user to use the entire set
# directly in a firewall rule and open up firewall to all
# of these applications. Also, the user should always
# specify the source and destination prefixes when using
# each application.
#
# NOTE: the contents of this set might grow in future JUNOS OS versions.
#
application-set junos-routing-inbound {
    application junos-bgp;
    application junos-rip;
    application junos-ldp-tcp;
    application junos-ldp-udp;
}
}
```

**Related  
Documentation**

- [Junos Default Groups on page 170](#)
- [Configuring Application Sets on page 163](#)
- [Configuring Application Protocol Properties on page 146](#)

---

## Configuring Application Protocol Properties

To configure application properties, include the **application** statement at the **[edit applications]** hierarchy level:

```
[edit applications]
application application-name {
    application-protocol protocol-name;
    destination-port port-number;
    icmp-code value;
    icmp-type value;
    inactivity-timeout value;
    protocol type;
    rpc-program-number number;
    snmp-command command;
    source-port port-number;
    ttl-threshold value;
    uuid hex-value;
}
```

You can group application objects by configuring the **application-set** statement; for more information, see “[Configuring Application Sets](#)” on page 163.

This section includes the following tasks for configuring applications:

- [Configuring an Application Protocol on page 147](#)
- [Configuring the Network Protocol on page 149](#)

- [Configuring the ICMP Code and Type on page 150](#)
- [Configuring Source and Destination Ports on page 152](#)
- [Configuring the Inactivity Timeout Period on page 155](#)
- [Configuring SIP on page 155](#)
- [Configuring an SNMP Command for Packet Matching on page 162](#)
- [Configuring an RPC Program Number on page 163](#)
- [Configuring the TTL Threshold on page 163](#)
- [Configuring a Universal Unique Identifier on page 163](#)

## Configuring an Application Protocol

The **application-protocol** statement allows you to specify which of the supported application protocols (ALGs) to configure and include in an application set for service processing. To configure application protocols, include the **application-protocol** statement at the **[edit applications application application-name]** hierarchy level:

```
[edit applications application application-name]
  application-protocol protocol-name;
```

[Table 19 on page 147](#) shows the list of supported protocols. For more information about specific protocols, see [“ALG Descriptions” on page 126](#).

**Table 19: Application Protocols Supported by Services Interfaces**

Protocol Name	CLI Value	Comments
Bootstrap protocol (BOOTP)	<b>bootp</b>	Supports BOOTP and dynamic host configuration protocol (DHCP).
Distributed Computing Environment (DCE) remote procedure call (RPC)	<b>dce-rpc</b>	Requires the <b>protocol</b> statement to have the value <b>udp</b> or <b>tcp</b> . Requires a <b>uuid</b> value. You cannot specify <b>destination-port</b> or <b>source-port</b> values.
DCE RPC portmap	<b>dce-rpc-portmap</b>	Requires the <b>protocol</b> statement to have the value <b>udp</b> or <b>tcp</b> . Requires a <b>destination-port</b> value.
Domain Name System (DNS)	<b>dns</b>	Requires the <b>protocol</b> statement to have the value <b>udp</b> . This application protocol closes the DNS flow as soon as the DNS response is received.
Exec	<b>exec</b>	Requires the <b>protocol</b> statement to have the value <b>tcp</b> or to be unspecified. Requires a <b>destination-port</b> value.
FTP	<b>ftp</b>	Requires the <b>protocol</b> statement to have the value <b>tcp</b> or to be unspecified. Requires a <b>destination-port</b> value.
H.323	<b>h323</b>	—
Internet Control Message Protocol (ICMP)	<b>icmp</b>	Requires the <b>protocol</b> statement to have the value <b>icmp</b> or to be unspecified.
Internet Inter-ORB Protocol	<b>iiop</b>	—
IP	<b>ip</b>	—

Table 19: Application Protocols Supported by Services Interfaces (*continued*)

Protocol Name	CLI Value	Comments
Login	<b>login</b>	—
NetBIOS	<b>netbios</b>	Requires the <b>protocol</b> statement to have the value <b>udp</b> or to be unspecified. Requires a <b>destination-port</b> value.
NetShow	<b>netshow</b>	Requires the <b>protocol</b> statement to have the value <b>tcp</b> or to be unspecified. Requires a <b>destination-port</b> value.
Point-to-Point Tunneling Protocol	<b>pptp</b>	—
RealAudio	<b>realaudio</b>	—
Real-Time Streaming Protocol (RTSP)	<b>rtsp</b>	Requires the <b>protocol</b> statement to have the value <b>tcp</b> or to be unspecified. Requires a <b>destination-port</b> value.
RPC User Datagram Protocol (UDP) or TCP	<b>rpc</b>	Requires the <b>protocol</b> statement to have the value <b>udp</b> or <b>tcp</b> . Requires a <b>rpc-program-number</b> value. You cannot specify <b>destination-port</b> or <b>source-port</b> values.
RPC port mapping	<b>rpc-portmap</b>	Requires the <b>protocol</b> statement to have the value <b>udp</b> or <b>tcp</b> . Requires a <b>destination-port</b> value.
Shell	<b>shell</b>	Requires the <b>protocol</b> statement to have the value <b>tcp</b> or to be unspecified. Requires a <b>destination-port</b> value.
Session Initiation Protocol	<b>sip</b>	—
SNMP	<b>snmp</b>	Requires the <b>protocol</b> statement to have the value <b>udp</b> or to be unspecified. Requires a <b>destination-port</b> value.
SQLNet	<b>sqlnet</b>	Requires the <b>protocol</b> statement to have the value <b>tcp</b> or to be unspecified. Requires a <b>destination-port</b> or <b>source-port</b> value.
Talk Program	<b>talk</b>	—
Trace route	<b>traceroute</b>	Requires the <b>protocol</b> statement to have the value <b>udp</b> or to be unspecified. Requires a <b>destination-port</b> value.
Trivial FTP (TFTP)	<b>tftp</b>	Requires the <b>protocol</b> statement to have the value <b>udp</b> or to be unspecified. Requires a <b>destination-port</b> value.
WinFrame	<b>winframe</b>	—



**NOTE:** You can configure application-level gateways (ALGs) for ICMP and trace route under stateful firewall, NAT, or CoS rules when twice NAT is configured in the same service set. These ALGs cannot be applied to flows created by the Packet Gateway Controller Protocol (PGCP). Twice NAT does not support any other ALGs. NAT applies only the IP address and TCP or UDP headers, but not the payload.

For more information about configuring twice NAT, see *Junos Address Aware Carrier Grade NAT and IPv6 Feature Guide*.

#### Related Documentation

- [ALGs Available by Default for Junos OS Address Aware NAT on page 62](#)

## Configuring the Network Protocol

The **protocol** statement allows you to specify which of the supported network protocols to match in an application definition. To configure network protocols, include the **protocol** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
protocol type;
```

You specify the protocol type as a numeric value; for the more commonly used protocols, text names are also supported in the command-line interface (CLI). [Table 20 on page 149](#) shows the list of the supported protocols.

**Table 20: Network Protocols Supported by Services Interfaces**

Network Protocol Type	CLI Value	Comments
IP Security (IPsec) authentication header (AH)	<b>ah</b>	—
External Gateway Protocol (EGP)	<b>egp</b>	—
IPsec Encapsulating Security Payload (ESP)	<b>esp</b>	—
Generic routing encapsulation (GR)	<b>gre</b>	—
ICMP	<b>icmp</b>	Requires an <b>application-protocol</b> value of <b>icmp</b> .
ICMPv6	<b>icmp6</b>	Requires an <b>application-protocol</b> value of <b>icmp</b> .
Internet Group Management Protocol (IGMP)	<b>igmp</b>	—
IP in IP	<b>ipip</b>	—
OSPF	<b>ospf</b>	—

Table 20: Network Protocols Supported by Services Interfaces (*continued*)

Network Protocol Type	CLI Value	Comments
Protocol Independent Multicast (PIM)	<b>pim</b>	—
Resource Reservation Protocol (RSVP)	<b>rsvp</b>	—
TCP	<b>tcp</b>	Requires a <b>destination-port</b> or <b>source-port</b> value unless you specify <b>application-protocol rcp</b> or <b>dce-rcp</b> .
UDP	<b>udp</b>	Requires a <b>destination-port</b> or <b>source-port</b> value unless you specify <b>application-protocol rcp</b> or <b>dce-rcp</b> .

For a complete list of possible numeric values, see RFC 1700, *Assigned Numbers (for the Internet Protocol Suite)*.



**NOTE:** IP version 6 (IPv6) is not supported as a network protocol in application definitions.

By default, the twice NAT feature can affect IP, TCP, and UDP headers embedded in the payload of ICMP error messages. You can include the **protocol tcp** and **protocol udp** statements with the application statement for twice NAT configurations. For more information about configuring twice NAT, see *Junos Address Aware Carrier Grade NAT and IPv6 Feature Guide*.

## Configuring the ICMP Code and Type

The ICMP code and type provide additional specification, in conjunction with the network protocol, for packet matching in an application definition. To configure ICMP settings, include the **icmp-code** and **icmp-type** statements at the **[edit applications application application-name]** hierarchy level:

```
[edit applications application application-name]
  icmp-code value;
  icmp-type value;
```

You can include only one ICMP code and type value. The **application-protocol** statement must have the value **icmp**. [Table 21 on page 151](#) shows the list of supported ICMP values.

Table 21: ICMP Codes and Types Supported by Services Interfaces

CLI Statement	Description
<b>icmp-code</b>	<p>This value or keyword provides more specific information than <b>icmp-type</b>. Because the value's meaning depends upon the associated <b>icmp-type</b> value, you must specify <b>icmp-type</b> along with <b>icmp-code</b>. For more information, see the <i>Routing Policy Feature Guide for Routing Devices</i>.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated:</p> <p>parameter-problem: <b>ip-header-bad</b> (0), <b>required-option-missing</b> (1)</p> <p>redirect: <b>redirect-for-host</b> (1), <b>redirect-for-network</b> (0), <b>redirect-for-tos-and-host</b> (3), <b>redirect-for-tos-and-net</b> (2)</p> <p>time-exceeded: <b>ttl-eq-zero-during-reassembly</b> (1), <b>ttl-eq-zero-during-transit</b> (0)</p> <p>unreachable: <b>communication-prohibited-by-filtering</b> (13), <b>destination-host-prohibited</b> (10), <b>destination-host-unknown</b> (7), <b>destination-network-prohibited</b> (9), <b>destination-network-unknown</b> (6), <b>fragmentation-needed</b> (4), <b>host-precedence-violation</b> (14), <b>host-unreachable</b> (1), <b>host-unreachable-for-TOS</b> (12), <b>network-unreachable</b> (0), <b>network-unreachable-for-TOS</b> (11), <b>port-unreachable</b> (3), <b>precedence-cutoff-in-effect</b> (15), <b>protocol-unreachable</b> (2), <b>source-host-isolated</b> (8), <b>source-route-failed</b> (5)</p>
<b>icmp-type</b>	<p>Normally, you specify this match in conjunction with the <b>protocol</b> match statement to determine which protocol is being used on the port. For more information, see the <i>Routing Policy Feature Guide for Routing Devices</i>.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): <b>echo-reply</b> (0), <b>echo-request</b> (8), <b>info-reply</b> (16), <b>info-request</b> (15), <b>mask-request</b> (17), <b>mask-reply</b> (18), <b>parameter-problem</b> (12), <b>redirect</b> (5), <b>router-advertisement</b> (9), <b>router-solicit</b> (10), <b>source-quench</b> (4), <b>time-exceeded</b> (11), <b>timestamp</b> (13), <b>timestamp-reply</b> (14), or <b>unreachable</b> (3).</p>



**NOTE:** If you configure an interface with an input firewall filter that includes a reject action and with a service set that includes stateful firewall rules, the router executes the input firewall filter before the stateful firewall rules are run on the packet. As a result, when the Packet Forwarding Engine sends an ICMP error message out through the interface, the stateful firewall rules might drop the packet because it was not seen in the input direction.

Possible workarounds are to include a forwarding-table filter to perform the reject action, because this type of filter is executed after the stateful firewall in the input direction, or to include an output service filter to prevent the locally generated ICMP packets from going to the stateful firewall service.

## Configuring Source and Destination Ports

The TCP or UDP source and destination port provide additional specification, in conjunction with the network protocol, for packet matching in an application definition. To configure ports, include the **destination-port** and **source-port** statements at the **[edit applications application application-name]** hierarchy level:

```
[edit applications application application-name]
destination-port value;
source-port value;
```

You must define one source or destination port. Normally, you specify this match in conjunction with the **protocol** match statement to determine which protocol is being used on the port; for constraints, see [Table 19 on page 147](#).

You can specify either a numeric value or one of the text synonyms listed in [Table 22 on page 152](#).

**Table 22: Port Names Supported by Services Interfaces**

Port Name	Corresponding Port Number
afs	1483
bgp	179
biff	512
bootpc	68
bootps	67
cmd	514
cvspserver	2401
dhcp	67
domain	53
eklogin	2105
ekshell	2106
exec	512
finger	79
ftp	21
ftp-data	20

Table 22: Port Names Supported by Services Interfaces (*continued*)

Port Name	Corresponding Port Number
http	80
https	443
ident	113
imap	143
kerberos-sec	88
klogin	543
kpasswd	761
krb-prop	754
krbupdate	760
kshell	544
ldap	389
login	513
mobileip-agent	434
mobileip-mn	435
msdp	639
netbios-dgm	138
netbios-ns	137
netbios-ssn	139
nfsd	2049
nntp	119
ntalk	518
ntp	123
pop3	110
pptp	1723

Table 22: Port Names Supported by Services Interfaces (*continued*)

Port Name	Corresponding Port Number
printer	515
radacct	1813
radius	1812
rip	520
rkinit	2108
smtp	25
snmp	161
snmptrap	162
snpp	444
socks	1080
ssh	22
sunrpc	111
syslog	514
tacacs-ds	65
talk	517
telnet	23
tftp	69
timed	525
who	513
xmcp	177
zephyr-clt	2103
zephyr-hm	2104

For more information about matching criteria, see the *Routing Policy Feature Guide for Routing Devices*.

## Configuring the Inactivity Timeout Period

You can specify a timeout period for application inactivity. If the software has not detected any activity during the duration, the flow becomes invalid when the timer expires. To configure a timeout period, include the **inactivity-timeout** statement at the **[edit applications application application-name]** hierarchy level:

```
[edit applications application application-name]
  inactivity-timeout seconds;
```

The default value is 30 seconds. The value you configure for an application overrides any global value configured at the **[edit interfaces interface-name service-options]** hierarchy level; for more information, see [“Configuring Default Timeout Settings for Services Interfaces” on page 799](#).

## Configuring SIP

The Session Initiation Protocol (SIP) is a generalized protocol for communication between endpoints involved in Internet services such as telephony, fax, video conferencing, instant messaging, and file exchange.

The Junos OS provides ALG services in accordance with the standard described in RFC 3261, *SIP: Session Initiation Protocol*. SIP flows under the Junos OS are as described in RFC 3665, *Session Initiation Protocol (SIP) Basic Call Flow Examples*.



**NOTE:** Before implementing the Junos OS SIP ALG, you should be familiar with certain limitations, discussed in [“Junos OS SIP ALG Limitations” on page 162](#)

The use of NAT in conjunction with the SIP ALG results in changes in SIP header fields due to address translation. For an explanation of these translations, refer to [“SIP ALG Interaction with Network Address Translation” on page 156](#).

To implement SIP on adaptive services interfaces, you configure the **application-protocol** statement at the **[edit applications application application-name]** hierarchy level with the value **sip**. For more information about this statement, see [“Configuring an Application Protocol” on page 147](#). In addition, there are two other statements you can configure to modify how SIP is implemented:

- You can enable the router to accept any incoming SIP calls for the endpoint devices that are behind the NAT firewall. When a device behind the firewall registers with the proxy that is outside the firewall, the AS or Multiservices PIC maintains the registration state. When the **learn-sip-register** statement is enabled, the router can use this information to accept inbound calls. If this statement is not configured, no inbound calls are accepted; only the devices behind the firewall can call devices outside the firewall.

To configure SIP registration, include the **learn-sip-register** statement at the **[edit applications application application-name]** hierarchy level:

```
[edit applications application application-name]  
learn-sip-register;
```

You can also manually inspect the SIP register by issuing the **show services stateful-firewall sip-register** command; for more information, see the *Junos OS System Basics and Services Command Reference*.

- You can specify a timeout period for the duration of SIP calls that are placed on hold. When a call is put on hold, there is no activity and flows might time out after the configured **inactivity-timeout** period expires, resulting in call state teardown. To avoid this, when a call is put on hold, the flow timer is reset to the **sip-call-hold-timeout** cycle to preserve the call state and flows for longer than the **inactivity-timeout** period.

To configure a timeout period, include the **sip-call-hold-timeout** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]  
sip-call-hold-timeout seconds;
```

The default value is 7200 seconds and the range is from 0 through 36,000 seconds (10 hours).

---

### SIP ALG Interaction with Network Address Translation

The Network Address Translation (NAT) protocol enables multiple hosts in a private subnet to share a single public IP address to access the Internet. For outgoing traffic, NAT replaces the private IP address of the host in the private subnet with the public IP address. For incoming traffic, the public IP address is converted back into the private address, and the message is routed to the appropriate host in the private subnet.

Using NAT with the Session Initiation Protocol (SIP) service is more complicated because SIP messages contain IP addresses in the SIP headers as well as in the SIP body. When using NAT with the SIP service, the SIP headers contain information about the caller and the receiver, and the device translates this information to hide it from the outside network. The SIP body contains the Session Description Protocol (SDP) information, which includes IP addresses and port numbers for transmission of the media. The device translates SDP information for allocating resources to send and receive the media.

How IP addresses and port numbers in SIP messages are replaced depends on the direction of the message. For an outgoing message, the private IP address and port number of the client are replaced with the public IP address and port number of the Juniper Networks firewall. For an incoming message, the public address of the firewall is replaced with the private address of the client.

When an INVITE message is sent out across the firewall, the SIP Application Layer Gateway (ALG) collects information from the message header into a call table, which it uses to forward subsequent messages to the correct endpoint. When a new message arrives, for example an ACK or 200 OK, the ALG compares the "From:", "To:", and "Call-ID:" fields against the call table to identify the call context of the message. If a new INVITE message arrives that matches the existing call, the ALG processes it as a REINVITE.

When a message containing SDP information arrives, the ALG allocates ports and creates a NAT mapping between them and the ports in the SDP. Because the SDP requires

sequential ports for the Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) channels, the ALG provides consecutive even-odd ports. If it is unable to find a pair of ports, it discards the SIP message.

This topic contains the following sections:

- [Outgoing Calls on page 157](#)
- [Incoming Calls on page 157](#)
- [Forwarded Calls on page 158](#)
- [Call Termination on page 158](#)
- [Call Re-INVITE Messages on page 158](#)
- [Call Session Timers on page 158](#)
- [Call Cancellation on page 159](#)
- [Forking on page 159](#)
- [SIP Messages on page 159](#)
- [SIP Headers on page 159](#)
- [SIP Body on page 161](#)

### ***Outgoing Calls***

When a SIP call is initiated with a SIP request message from the internal to the external network, NAT replaces the IP addresses and port numbers in the SDP and binds the IP addresses and port numbers to the Juniper Networks firewall. Via, Contact, Route, and Record-Route SIP header fields, if present, are also bound to the firewall IP address. The ALG stores these mappings for use in retransmissions and for SIP response messages.

The SIP ALG then opens pinholes in the firewall to allow media through the device on the dynamically assigned ports negotiated based on information in the SDP and the Via, Contact, and Record-Route header fields. The pinholes also allow incoming packets to reach the Contact, Via, and Record-Route IP addresses and ports. When processing return traffic, the ALG inserts the original Contact, Via, Route, and Record-Route SIP fields back into packets.

### ***Incoming Calls***

Incoming calls are initiated from the public network to public static NAT addresses or to interface IP addresses on the device. Static NATs are statically configured IP addresses that point to internal hosts; interface IP addresses are dynamically recorded by the ALG as it monitors REGISTER messages sent by internal hosts to the SIP registrar. When the device receives an incoming SIP packet, it sets up a session and forwards the payload of the packet to the SIP ALG.

The ALG examines the SIP request message (initially an INVITE) and, based on information in the SDP, opens gates for outgoing media. When a 200 OK response message arrives, the SIP ALG performs NAT on the IP addresses and ports and opens pinholes in the outbound direction. (The opened gates have a short time-to-live, and they time out if a 200 OK response message is not received quickly.)

When a 200 OK response arrives, the SIP proxy examines the SDP information and reads the IP addresses and port numbers for each media session. The SIP ALG on the device performs NAT on the addresses and port numbers, opens pinholes for outbound traffic, and refreshes the timeout for gates in the inbound direction.

When the ACK arrives for the 200 OK, it also passes through the SIP ALG. If the message contains SDP information, the SIP ALG ensures that the IP addresses and port numbers are not changed from the previous INVITE—if they are, the ALG deletes old pinholes and creates new pinholes to allow media to pass through. The ALG also monitors the Via, Contact, and Record-Route SIP fields and opens new pinholes if it determines that these fields have changed.

### ***Forwarded Calls***

A forwarded call is when, for example, user A outside the network calls user B inside the network, and user B forwards the call to user C outside the network. The SIP ALG processes the INVITE from user A as a normal incoming call. But when the ALG examines the forwarded call from B to C outside the network and notices that B and C are reached using the same interface, it does not open pinholes in the firewall, because media will flow directly between user A and user C.

### ***Call Termination***

The BYE message terminates a call. When the device receives a BYE message, it translates the header fields just as it does for any other message. But because a BYE message must be acknowledged by the receiver with a 200 OK, the ALG delays call teardown for five seconds to allow time for transmission of the 200 OK.

### ***Call Re-INVITE Messages***

Re-INVITE messages add new media sessions to a call and remove existing media sessions. When new media sessions are added to a call, new pinholes are opened in the firewall and new address bindings are created. The process is identical to the original call setup. When one or more media sessions are removed from a call, pinholes are closed and bindings released just as with a BYE message.

### ***Call Session Timers***

The SIP ALG uses the Session-Expires value to time out a session if a Re-INVITE or UPDATE message is not received. The ALG gets the Session-Expires value, if present, from the 200 OK response to the INVITE and uses this value for signaling timeout. If the ALG receives another INVITE before the session times out, it resets all timeout values to this new INVITE or to default values, and the process is repeated.

As a precautionary measure, the SIP ALG uses hard timeout values to set the maximum amount of time a call can exist. This ensures that the device is protected should one of the following events occur:

- End systems crash during a call and a BYE message is not received.
- Malicious users never send a BYE in an attempt to attack a SIP ALG.

- Poor implementations of SIP proxy fail to process Record-Route and never send a BYE message.
- Network failures prevent a BYE message from being received.

### ***Call Cancellation***

Either party can cancel a call by sending a CANCEL message. Upon receiving a CANCEL message, the SIP ALG closes pinholes through the firewall—if any have been opened—and releases address bindings. Before releasing the resources, the ALG delays the control channel age-out for approximately five seconds to allow time for the final 200 OK to pass through. The call is terminated when the five second timeout expires, regardless of whether a 487 or non-200 response arrives.

### ***Forking***

Forking enables a SIP proxy to send a single INVITE message to multiple destinations simultaneously. When the multiple 200 OK response messages arrive for the single call, the SIP ALG parses but updates call information with the first 200 OK messages it receives.

### ***SIP Messages***

The SIP message format consists of a SIP header section and the SIP body. In request messages, the first line of the header section is the request line, which includes the method type, request-URI, and protocol version. In response messages, the first line is the status line, which contains a status code. SIP headers contain IP addresses and port numbers used for signaling. The SIP body, separated from the header section by a blank line, is reserved for session description information, which is optional. Junos OS currently supports the SDP only. The SIP body contains IP addresses and port numbers used to transport the media.

### ***SIP Headers***

In the following sample SIP request message, NAT replaces the IP addresses in the header fields to hide them from the outside network.

```
INVITE bob@10.150.20.5 SIP/2.0
Via: SIP/2.0/UDP 10.150.20.3:5434
From: alice@10.150.20.3
To: bob@10.150.20.5
Call-ID: a12abcde@10.150.20.3
Contact: alice@10.150.20.3:5434
Route: <sip:netscreen@10.150.20.3:5060>
Record-Route: <sip:netscreen@10.150.20.3:5060>
```

How IP address translation is performed depends on the type and direction of the message. A message can be any of the following:

- Inbound request
- Outbound response
- Outbound request
- Inbound response

Table 23 on page 160 shows how NAT is performed in each of these cases. Note that for several of the header fields the ALG determine more than just whether the messages comes from inside or outside the network. It must also determine what client initiated the call, and whether the message is a request or response.

**Table 23: Requesting Messages with NAT Table**

Inbound Request (from public to private)	To:	Replace domain with local address
	From:	None
	Call-ID:	None
	Via:	None
	Request-URI:	Replace ALG address with local address
	Contact:	None
	Record-Route:	None
	Route:	None
Outbound Response (from private to public)	To:	Replace ALG address with local address
	From:	None
	Call-ID:	None
	Via:	None
	Request-URI:	N/A
	Contact:	Replace local address with ALG address
	Record-Route:	Replace local address with ALG address
	Route:	None

Table 23: Requesting Messages with NAT Table (*continued*)

Outbound Request (from private to public)	To:	None
	From:	Replace local address with ALG address
	Call-ID:	None
	Via:	Replace local address with ALG address
	Request-URI:	None
	Contact:	Replace local address with ALG address
	Record-Route:	Replace local address with ALG address
	Route:	Replace ALG address with local address
Outbound Response (from public to private)	To:	None
	From:	Replace ALG address with local address
	Call-ID:	None
	Via:	Replace ALG address with local address
	Request-URI:	N/A
	Contact:	None
	Record-Route:	Replace ALG address with local address
	Route:	Replace ALG address with local address

***SIP Body***

The SDP information in the SIP body includes IP addresses the ALG uses to create channels for the media stream. Translation of the SDP section also allocates resources, that is, port numbers to send and receive the media.

The following excerpt from a sample SDP section shows the fields that are translated for resource allocation.

```
o=user 2344234 55234434 IN IP4 10.150.20.3
c=IN IP4 10.150.20.3
m=audio 43249 RTP/AVP 0
```

SIP messages can contain more than one media stream. The concept is similar to attaching multiple files to an e-mail message. For example, an INVITE message sent from a SIP client to a SIP server might have the following fields:

```
c=IN IP4 10.123.33.4
m=audio 33445 RTP/AVP 0
```

```
c=IN IP4 10.123.33.4
m=audio 33447 RTP/AVP 0
c=IN IP4 10.123.33.4
m=audio 33449 RTP/AVP 0
```

Junos OS supports up to 6 SDP channels negotiated for each direction, for a total of 12 channels per call. For more information, see *SDP Session Descriptions*.

---

### Junos OS SIP ALG Limitations

The following limitations apply to configuration of the SIP ALG:

- Only the methods described in RFC 3261 are supported.
- Only SIP version 2 is supported.
- TCP is not supported as a transport mechanism for signaling messages.
- *Do not configure the SIP ALG when using STUN.* If clients use STUN/TURN to detect the firewall or NAT devices between the caller and responder or proxy, the client attempts to best-guess the NAT device behavior and act accordingly to place the call.
- Do not use the endpoint-independent mapping NAT pool option in conjunction with the SIP ALG. Errors will result.
- IPv6 signaling data is not supported.
- Authentication is not supported.
- Encrypted messages are not supported.
- SIP fragmentation is not supported.
- The maximum UDP packet size containing a SIP message is assumed to be 4 KB. SIP messages larger than this are not supported.
- The maximum number of media channels in a SIP message is assumed to be six.
- Fully qualified domain names (FQDNs) are not supported in critical fields.
- QoS is not supported.
- High availability is not supported, except for warm standby.
- A timeout setting of never is not supported on SIP or NAT.
- Multicast (forking proxy) is not supported.

### Configuring an SNMP Command for Packet Matching

You can specify an SNMP command setting for packet matching. To configure SNMP, include the **snmp-command** statement at the **[edit applications application application-name]** hierarchy level:

```
[edit applications application application-name]
  snmp-command value;
```

The supported values are **get**, **get-next**, **set**, and **trap**. You can configure only one value for matching. The **application-protocol** statement at the **[edit applications application**

**application-name**] hierarchy level must have the value **snmp**. For information about specifying the application protocol, see [“Configuring an Application Protocol” on page 147](#).

## Configuring an RPC Program Number

You can specify an RPC program number for packet matching. To configure an RPC program number, include the **rpc-program-number** statement at the **[edit applications application application-name]** hierarchy level:

```
[edit applications application application-name]
  rpc-program-number number;
```

The range of values used for DCE or RPC is from 100,000 through 400,000. The **application-protocol** statement at the **[edit applications application application-name]** hierarchy level must have the value **rpc**. For information about specifying the application protocol, see [“Configuring an Application Protocol” on page 147](#).

## Configuring the TTL Threshold

You can specify a trace route time-to-live (TTL) threshold value, which controls the acceptable level of network penetration for trace routing. To configure a TTL value, include the **ttl-threshold** statement at the **[edit applications application application-name]** hierarchy level:

```
[edit applications application application-name]
  ttl-threshold value;
```

The **application-protocol** statement at the **[edit applications application application-name]** hierarchy level must have the value **traceroute**. For information about specifying the application protocol, see [“Configuring an Application Protocol” on page 147](#).

## Configuring a Universal Unique Identifier

You can specify a Universal Unique Identifier (UUID) for DCE RPC objects. To configure a UUID value, include the **uuid** statement at the **[edit applications application application-name]** hierarchy level:

```
[edit applications application application-name]
  uuid hex-value;
```

The **uuid** value is in hexadecimal notation. The **application-protocol** statement at the **[edit applications application application-name]** hierarchy level must have the value **dce-rpc**. For information about specifying the application protocol, see [“Configuring an Application Protocol” on page 147](#). For more information on UUID numbers, see <http://www.opengroup.org/onlinepubs/9629399/apdx.htm>.

## Configuring Application Sets

You can group the applications you have defined into a named object by including the **application-set** statement at the **[edit applications]** hierarchy level with an **application** statement for each application:

```
[edit applications]
  application-set application-set-name {
```

```

    application application;
}

```

For an example of a typical application set, see “Examples: Configuring Application Protocols” on page 177.

#### Related Documentation

- [ALG Descriptions on page 126](#)
- [Configuring Application Protocol Properties on page 146](#)
- [Examples: Configuring Application Protocols on page 177](#)
- [Verifying the Output of ALG Sessions on page 164](#)

## Verifying the Output of ALG Sessions

This section contains examples of successful output from ALG sessions and information on system log configuration. You can compare the results of your sessions to check whether the configurations are functioning correctly.

- [FTP Example on page 164](#)
- [RTSP ALG Example on page 167](#)
- [System Log Messages on page 169](#)

### FTP Example

This example analyzes the output during an active FTP session. It consists of four different flows; two are control flows and two are data flows. The example consists of the following parts:

- [Sample Output on page 164](#)
- [FTP System Log Messages on page 165](#)
- [Analysis on page 166](#)
- [Troubleshooting Questions on page 166](#)

#### Sample Output

The following is a complete sample output from the **show services stateful-firewall conversations application-protocol ftp** operational mode command:

```

user@host>show services stateful-firewall conversations application-protocol ftp
Interface: ms-1/3/0, Service set: CLBJI1-AAF001
Conversation: ALG protocol: ftp
  Number of initiators: 2, Number of responders: 2
Flow      State  Dir      Frm count
TCP       1.1.79.2:14083 -> 2.2.2.2:21 Watch I      13
  NAT source      1.1.79.2:14083 -> 194.250.1.237:50118
TCP       1.1.79.2:14104 -> 2.2.2.2:20 Forward I      3
  NAT source      1.1.79.2:14104 -> 194.250.1.237:50119
TCP       2.2.2.2:21 -> 194.250.1.237:50118 Watch O      12
  NAT dest        194.250.1.237:50118 -> 1.1.79.2:14083
TCP       2.2.2.2:20 -> 194.250.1.237:50119 Forward O      5
  NAT dest        194.250.1.237:50119 -> 1.1.79.2:14104

```

For each flow, the first line shows flow information, including protocol (TCP), source address, source port, destination address, destination port, flow state, direction, and frame count.

- The state of a flow can be **Watch**, **Forward**, or **Drop**:
  - A **Watch** flow state indicates that the control flow is monitored by the ALG for information in the payload. NAT processing is performed on the header and payload as needed.
  - A **Forward** flow forwards the packets without monitoring the payload. NAT is performed on the header as needed.
  - A **Drop** flow drops any packet that matches the 5 tuple.
- The frame count (**Frm count**) shows the number of packets that were processed on that flow.

The second line shows the NAT information.

- **source** indicates source NAT.
- **dest** indicates destination NAT.
- The first address and port in the NAT line are the original address and port being translated for that flow.
- The second address and port in the NAT line are the translated address and port for that flow.

### FTP System Log Messages

System log messages are generated during an FTP session. For more information about system logs, see [“System Log Messages” on page 169](#).

The following system log messages are generated during creation of the FTP control flow:

- Rule Accept system log:
 

```
Oct 27 11:42:54 (FPC Slot 1, PIC Slot 1) {ss_ftp}[FWNAT]: ASP_SFW_RULE_ACCEPT:
proto 6 (TCP) application: ftp, fe-3/3/3.0:1.1.1.2:4450 -> 2.2.2.2:21, Match SFW accept
rule-set:, rule: ftp, term: 1
```
- Create Accept Flow system log:
 

```
Oct 27 11:42:54 (FPC Slot 1, PIC Slot 1) {ss_ftp}[FWNAT]:
ASP_SFW_CREATE_ACCEPT_FLOW: proto 6 (TCP) application: ftp,
fe-3/3/3.0:1.1.1.2:4450 -> 2.2.2.2:21, creating forward or watch flow
```
- System log for data flow creation:
 

```
Oct 27 11:43:30 (FPC Slot 1, PIC Slot 1) {ss_ftp}[FWNAT]:
ASP_SFW_FTP_ACTIVE_ACCEPT: proto 6 (TCP) application: ftp, so-2/1/2.0:2.2.2.2:20
-> 1.1.1.2:50726, Creating FTP active mode forward flow
```

## Analysis

### Control Flows

The control flows are established after the three-way handshake is complete.

- Control flow from FTP client to FTP server. TCP destination port is 21.

```
TCP      1.1.79.2:14083 ->      2.2.2.2:21    Watch    I
13
NAT source      1.1.79.2:14083 ->    194.250.1.237:50118
```

- Control flow from FTP server to FTP client. TCP source port is 21.

```
TCP      2.2.2.2:21    ->    194.250.1.237:50118 Watch    O
12
NAT dest      194.250.1.237:50118 ->      1.1.79.2:14083
```

### Data Flows

A data port of 20 is negotiated for data transfer during the course of the FTP control protocol. These two flows are data flows between the FTP client and the FTP server:

```
TCP      1.1.79.2:14104 ->      2.2.2.2:20    Forward  I           3
NAT source      1.1.79.2:14104 ->    194.250.1.237:50119
TCP      2.2.2.2:20    ->    194.250.1.237:50119 Forward  O           5
NAT dest      194.250.1.237:50119 ->      1.1.79.2:14104
```

## Troubleshooting Questions

- How do I know if the FTP ALG is active?
  - The ALG protocol field in the conversation should display **ftp**.
  - There should be a valid frame count (**Frm count**) in the control flows.
  - A valid frame count in the data flows indicates that data transfer has taken place.
- What do I need to check if the FTP connection is established but data transfer does not take place?
  - Most probably, the control connection is up, but the data connection is down.
  - Check the conversations output to determine whether both the control and data flows are present.
- How do I interpret each flow? What does each flow mean?
  - FTP control flow initiator flow—Flow with destination port 21
  - FTP control flow responder flow—Flow with source port ;21
  - FTP data flow initiator flow—Flow with destination port 20
  - FTP data flow responder flow—Flow with source port 20

## RTSP ALG Example

The following is an example of an RTSP conversation. The application uses the RTSP protocol for control connection. Once the connection is set up, the media is sent using UDP protocol (RTP).

This example consists of the following:

- [Sample Output on page 167](#)
- [Analysis on page 167](#)
- [Troubleshooting Questions on page 167](#)

### Sample Output

Here is the output from the **show services stateful-firewall conversations** operational mode command:

```
user@host# show services stateful-firewall conversations
Interface: ms-3/2/0, Service set: svc_set
Conversation: ALG protocol: rtsp
Number of initiators: 5, Number of responders: 5
```

Flow			State	Dir	Frm count	
TCP	1.1.1.3:58795	->	2.2.2.2:554	Watch	I	7
UDP	1.1.1.3:1028	->	2.2.2.2:1028	Forward	I	0
UDP	1.1.1.3:1029	->	2.2.2.2:1029	Forward	I	0
UDP	1.1.1.3:1030	->	2.2.2.2:1030	Forward	I	0
UDP	1.1.1.3:1031	->	2.2.2.2:1031	Forward	I	0
TCP	2.2.2.2:554	->	1.1.1.3:58795	Watch	O	5
UDP	2.2.2.2:1028	->	1.1.1.3:1028	Forward	O	6
UDP	2.2.2.2:1029	->	1.1.1.3:1029	Forward	O	0
UDP	2.2.2.2:1030	->	1.1.1.3:1030	Forward	O	3
UDP	2.2.2.2:1031	->	1.1.1.3:1031	Forward	O	0

### Analysis

An RTSP conversation should consist of TCP flows corresponding to the RTSP control connection. There should be two flows, one in each direction, from client to server and from server to client:

TCP	1.1.1.3:58795	->	2.2.2.2:554	Watch	I	7
TCP	2.2.2.2:554	->	1.1.1.3:58795	Watch	O	5

- The RTSP control connection for the initiator flow is sent from destination port 554.
- The RTSP control connection for the responder flow is sent from source port 554.

The UDP flows correspond to RTP media sent over the RTSP connection.

### Troubleshooting Questions

- Media does not work when the RTSP ALG is configured. What do I do?
  - Check RTSP conversations to see whether both TCP and UDP flows exist.
  - The ALG protocol should be displayed as **rtsp**.



**NOTE:** The state of the flow is displayed as **Watch**, because the ALG processing is taking place and the client is essentially “watching” or processing payload corresponding to the application. For FTP and RTSP ALG flows, the control connections are always Watch flows.

## 2. How do I check for ALG errors?

- You can check for errors by issuing the following command. Each ALG has a separate field for ALG packet errors.

```
user@host# show services stateful-firewall statistics extensive
Interface: ms-3/2/0
Service set: svc_set
New flows:
  Accepts: 1347, Discards: 0, Rejects: 0
Existing flows:
  Accepts: 144187, Discards: 0, Rejects: 0
Drops:
  IP option: 0, TCP SYN defense: 0
  NAT ports exhausted: 0
Errors:
  IP: 0, TCP: 276
  UDP: 0, ICMP: 0
  Non-IP packets: 0, ALG: 0
IP errors:
  IP packet length inconsistencies: 0
  Minimum IP header length check failures: 0
  Reassembled packet exceeds maximum IP length: 0
  Illegal source address: 0
  Illegal destination address: 0
  TTL zero errors: 0, Illegal IP protocol number (0 or 255): 0
  Land attack: 0
  Non-IPv4 packets: 0, Bad checksum: 0
  Illegal IP fragment length: 0
  IP fragment overlap: 0
  IP fragment reassembly timeout: 0
  Unknown: 0
TCP errors:
  TCP header length inconsistencies: 0
  Source or destination port number is zero: 0
  Illegal sequence number and flags combinations: 0
  SYN attack (multiple SYN messages seen for the same flow): 276
  First packet not a SYN message: 0
  TCP port scan (TCP handshake, RST seen from server for SYN): 0
  Bad SYN cookie response: 0
UDP errors:
  IP data length less than minimum UDP header length (8 bytes): 0
  Source or destination port number is zero: 0
  UDP port scan (ICMP error seen for UDP flow): 0
ICMP errors:
  IP data length less than minimum ICMP header length (8 bytes): 0
  ICMP error length inconsistencies: 0
  Duplicate ping sequence number: 0
  Mismatched ping sequence number: 0
ALG errors:
  BOOTP: 0, DCE-RPC: 0, DCE-RPC portmap: 0
  DNS: 0, Exec: 0, FTP: 0
  ICMP: 0
```

```

Login: 0, NetBIOS: 0, NetShow: 0
RPC: 0, RPC portmap: 0
RTSP: 0, Shell: 0
SNMP: 0, SQLNet: 0, TFTP: 0
Traceroute: 0

```

## System Log Messages

Enabling system log generation and checking the system log are also helpful for ALG flow analysis. This section contains the following:

- [System Log Configuration on page 169](#)
- [System Log Output on page 170](#)

### System Log Configuration

You can configure the enabling of system log messages at a number of different levels in the Junos OS CLI. As shown in the following sample configurations, the choice of level depends on how specific you want the event logging to be and what options you want to include. For details on the configuration options, see the *Junos OS Administration Library for Routing Devices* (system level) or the *Junos OS Services Interfaces Library for Routing Devices* (all other levels).

1. At the topmost global level:

```

user@host# show system syslog
file messages {
    any any;
}

```

2. At the service set level:

```

user@host# show services service-set svc_set
syslog {
    host local {
        services any;
    }
}
stateful-firewall-rules allow_rtsp;
interface-service {
    service-interface ms-3/2/0;
}

```

3. At the service rule level:

```

user@host# show services stateful-firewall rule allow_rtsp
match-direction input-output;
term 0 {
    from {
        applications junos-rtsp;
    }
    then {
        accept;
        syslog;
    }
}

```

## System Log Output

---

System log messages are generated during flow creation, as shown in the following examples:

The following system log message indicates that the ASP matched an accept rule:

```
Oct 25 16:11:37 (FPC Slot 3, PIC Slot 2) {svc_set}[FWNAT]: ASP_SFW_RULE_ACCEPT:
proto 6 (TCP) application: rtsp, ge-2/0/1.0:1.1.1.2:35595 -> 2.2.2.2:554, Match SFW accept
rule-set: , rule: allow_rtsp, term: 0
```

For a complete listing of system log messages, see the *Junos OS System Log Messages Reference*.

### Related Documentation

- [ALG Descriptions on page 126](#)
- [Configuring Application Sets on page 163](#)
- [Configuring Application Protocol Properties on page 146](#)
- [Examples: Configuring Application Protocols on page 177](#)

## Junos Default Groups

---

The Junos OS provides a default, hidden configuration group called **junos-defaults** that is automatically applied to the configuration of your router. The **junos-defaults** group contains preconfigured statements that contain predefined values for common applications. Some of the statements must be referenced to take effect, such as applications like FTP or Telnet. Other statements are applied automatically, such as terminal settings. All of the preconfigured statements begin with the reserved name **junos-**.



**NOTE:** You can override the Junos default configuration values, but you cannot delete or edit them. If you delete a configuration, the defaults return when a new configuration is added.

You cannot use the **apply-groups** statement with the Junos defaults group.

To view the full set of available preset statements from the Junos default group, issue the **show groups junos-defaults** configuration mode command. The following example displays a partial list of Junos default groups that use application protocols (ALGs).

```
user@host# show groups junos-defaults
... output for other groups defined at the [edit groups junos-defaults] hierarchy level ...
applications {
  # File Transfer Protocol
  application junos-ftp {
    application-protocol ftp;
    protocol tcp;
    destination-port 21;
  }
}
```

```
# Trivial File Transfer Protocol
application junos-tftp {
    application-protocol tftp;
    protocol udp;
    destination-port 69;
}
# RPC port mapper on TCP
application junos-rpc-portmap-tcp {
    application-protocol rpc-portmap;
    protocol tcp;
    destination-port 111;
}
# RPC port mapper on UDP
application junos-rpc-portmap-udp {
    application-protocol rpc-portmap;
    protocol udp;
    destination-port 111;
}
# IP Protocol
application junos-ip {
    application-protocol ip;
}
# remote exec
application junos-rexec {
    application-protocol exec;
    protocol tcp;
    destination-port 512;
}
# remote login
application junos-rlogin {
    application-protocol login;
    protocol tcp;
    destination-port 513;
}
# remote shell
application junos-rsh {
    application-protocol shell;
    protocol tcp;
    destination-port 514;
}
# Real-Time Streaming Protocol
application junos-rtsp {
    application-protocol rtsp;
    protocol tcp;
    destination-port 554;
}
# Oracle SQL servers use this protocol to execute SQL commands
# from clients, load balance, use application-specific servers, and so on.
application junos-sqlnet {
    application-protocol sqlnet;
    protocol tcp;
    destination-port 1521;
}
# H.323 Protocol for audio/video conferencing
protocol tcp;
    destination-port 1720;
```

```
}
# Internet Inter-ORB Protocol is used for CORBA applications.
# The ORB protocol in Java virtual machine uses port 1975 as a default.
protocol tcp;
  destination-port 1975;
}
# Internet Inter-ORB Protocol is used for CORBA applications.
# ORBIX is a CORBA framework from Iona Technologies that uses
# port 3075 as a default.
protocol tcp;
  destination-port 3075;
}
# This was the original RealPlayer protocol.
# RTSP is more widely used by RealPlayer,
protocol tcp;
  destination-port 7070;
}
# Traceroute application
application junos-traceroute {
  application-protocol traceroute;
  protocol udp;
  destination-port 33435-33450;
  ttl-threshold 30;
}
# Traceroute application that stops at device supporting firewall
# (packets with ttl > 1 will be discarded).
application junos-traceroute-ttl-1 {
  application-protocol traceroute;
  protocol udp;
  destination-port 33435-33450;
  ttl-threshold 1;
}
# The full range of known RPC programs using UDP.
# Specific program numbers are assigned to certain applications.
application junos-rpc-services-udp {
  application-protocol rpc;
  protocol udp;
  rpc-program-number 100001-400000;
}
# The full range of known RPC programs using TCP.
# Specific program numbers are assigned to certain applications.
application junos-rpc-services-tcp {
  application-protocol rpc;
  protocol tcp;
  rpc-program-number 100001-400000;
}
# All ICMP traffic
# This can be made more restrictive by specifying ICMP type and code.
application junos-icmp-all {
  application-protocol icmp;
}
# ICMP ping; the echo reply is allowed upon return.
application junos-icmp-ping {
  application-protocol icmp;
  icmp-type echo-request;
}
```

```
# Protocol used by Windows Media Server and Windows Media Player
application junos-netshow {
    application-protocol netshow;
    protocol tcp;
    destination-port 1755;
}
# NetBIOS, the networking protocol used on Windows networks;
# includes name service port, both UDP and TCP.
application junos-netbios-name-udp {
    application-protocol netbios;
    protocol udp;
    destination-port 137;
}
application junos-netbios-name-tcp {
    protocol tcp;
    destination-port 137;
}
# NetBIOS, the networking protocol used on Windows networks;
# includes datagram service port.
application junos-netbios-datagram {
    application-protocol netbios;
    protocol udp;
    destination-port 138;
}
# NetBIOS, the networking protocol used on Windows networks;
# includes session service port.
application junos-netbios-session {
    protocol tcp;
    destination-port 139;
}
# DCE-RPC port mapper on TCP
application junos-dce-rpc-portmap {
    application-protocol dce-rpc-portmap;
    protocol tcp;
    destination-port 135;
}
# MS Exchange requires these three UUID values.
application junos-dcerpc-endpoint-mapper-service {
    application-protocol dce-rpc;
    protocol tcp;
    uuid e1af8308-5d1f-11c9-91a4-08002b14a0fa;
}
application junos-ssh {
    protocol tcp;
    destination-port 22;
}
application junos-telnet {
    protocol tcp;
    destination-port 23;
}
application junos-smtp {
    protocol tcp;
    destination-port 25;
}
application junos-dns-udp {
    protocol udp;
```

```
        destination-port 53;
    }
    application junos-dns-tcp {
        protocol tcp;
        destination-port 53;
    }
    application junos-tacacs {
        protocol tcp;
        destination-port 49;
    }
    # TACACS Database Service
    application junos-tacacs-ds {
        protocol tcp;
        destination-port 65;
    }
    application junos-dhcp-client {
        protocol udp;
        destination-port 68;
    }
    application junos-dhcp-server {
        protocol udp;
        destination-port 67;
    }
    application junos-bootpc {
        protocol udp;
        destination-port 68;
    }
    application junos-bootps {
        protocol udp;
        destination-port 67;
    }
    application junos-http {
        protocol tcp;
        destination-port 80;
    }
    application junos-https {
        protocol tcp;
        destination-port 443;
    }
    # "junos-algs-outbound" defines a set of all applications
    # requiring an ALG. Useful for defining a rule for an untrusted
    # network to allow trusted network users to use all the
    # Junos-supported ALGs initiated from the trusted network.
    application-set junos-algs-outbound {
        application junos-ftp;
        application junos-tftp;
        application junos-rpc-portmap-tcp;
        application junos-rpc-portmap-udp;
        application junos-snmp-get;
        application junos-snmp-get-next;
        application junos-snmp-response;
        application junos-snmp-trap;
        application junos-rexec;
        application junos-rlogin;
        application junos-rsh;
        application junos-rtsp;
```

```

application junos-sqlnet;
application junos-traceroute;
application junos-rpc-services-udp;
application junos-rpc-services-tcp;
application junos-icmp-all;
application junos-netshow;
application junos-netbios-name-udp;
application junos-netbios-datagram;
application junos-dce-rpc-portmap;
application junos-dcerpc-msexchange-directory-rfr;
application junos-dcerpc-msexchange-information-store;
application junos-dcerpc-msexchange-directory-nsp;
}
# " junos-management-inbound" represents the group of applications
# that might need access to the trusted network from the untrusted
# network for management purposes.
# The set is intended for a UI to display management choices.
# NOTE: It is not recommended that you use the entire set directly in
# a firewall rule and open up firewall to all of these
# applications. Also, you should always specify the source
# and destination prefixes when using each application.
application-set junos-management-inbound {
    application junos-snmp-get;
    application junos-snmp-get-next;
    application junos-snmp-response;
    application junos-snmp-trap;
    application junos-ssh;
    application junos-telnet;
    application junos-http;
    application junos-https;
    application junos-xnm-ssl;
    application junos-xnm-clear-text;
    application junos-icmp-ping;
    application junos-traceroute-ttl-1;
}
}
}
}

```

To reference statements available from the **junos-defaults** group, include the selected **junos-default-name** statement at the applicable hierarchy level. To configure application protocols, see [“Configuring Application Protocol Properties” on page 146](#); for details about a specific protocol, see [“ALG Descriptions” on page 126](#).

## Examples: Referencing the Preset Statement from the Junos Default Group

The following example is a preset statement from the Junos default groups that is available for FTP in a stateful firewall:

```

[edit]
groups {
    junos-defaults {
        applications {
            application junos-ftp { # Use FTP default configuration
                application-protocol ftp;
                protocol tcp;
            }
        }
    }
}

```

```
        destination-port 21;
    }
}
```

To reference a preset Junos default statement from the Junos default groups, include the **junos-default-name** statement at the applicable hierarchy level. For example, to reference the Junos default statement for FTP in a stateful firewall, include the **junos-ftp** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* from applications]** hierarchy level.

```
[edit]
services {
  stateful-firewall {
    rule my-rule {
      term my-term {
        from {
          applications junos-ftp; #Reference predefined statement, junos-ftp,
        }
      }
    }
  }
}
```

The following example shows configuration of the default Junos IP ALG:

```
[edit]
services {
  stateful-firewall {
    rule r1 {
      match-direction input;
      term t1 {
        from {
          applications junos-ip;
        }
        then {
          accept;
          syslog;
        }
      }
    }
  }
}
```

If you configure the IP ALG in the stateful firewall rule, it is matched by any IP traffic, but if there is any other more specific application that matches the same traffic, the IP ALG will not be matched. For example, in the following configuration, both the ICMP ALG and the IP ALG are configured, but traffic is matched for ICMP packets, because it is the more specific match.

```
[edit]
services {
  stateful-firewall {
    rule r1 {
      match-direction input;
      term t1 {
```

```

        from {
            applications [ junos-ip junos-icmp-all ];
        }
        then {
            accept;
            syslog;
        }
    }
}
}

```

**Related  
Documentation**

- [ALG Descriptions on page 126](#)
- [Configuring Application Sets on page 163](#)
- [Configuring Application Protocol Properties on page 146](#)

## Examples: Configuring Application Protocols

The following example shows an application protocol definition describing a special FTP application running on port 78:

```

[edit applications]
application my-ftp-app {
    application-protocol ftp;
    protocol tcp;
    destination-port 78;
    timeout 100; # inactivity timeout for FTP service
}

```

The following example shows a special ICMP protocol (**application-protocol icmp**) of type 8 (ICMP echo):

```

[edit applications]
application icmp-app {
    application-protocol icmp;
    protocol icmp;
    icmp-type icmp-echo;
}

```

The following example shows a possible application set:

```

[edit applications]
application-set basic {
    http;
    ftp;
    telnet;
    nfs;
    icmp;
}

```

The software includes a predefined set of well-known application protocols. The set includes applications for which the TCP and UDP destination ports are already recognized by stateless firewall filters.

- Related Documentation**
- [ALG Descriptions on page 126](#)
  - [Configuring Application Sets on page 163](#)
  - [Configuring Application Protocol Properties on page 146](#)
  - [Verifying the Output of ALG Sessions on page 164](#)

## CHAPTER 5

# Summary of Applications Configuration Statements

The following sections explain each of the applications configuration statements. The statements are organized alphabetically.

## application

---

Syntax	<pre>application <i>application-name</i> {   application-protocol <i>protocol-name</i>;   destination-port <i>port-number</i>;   icmp-code <i>value</i>;   icmp-type <i>value</i>;   inactivity-timeout <i>value</i>;   protocol <i>type</i>;   rpc-program-number <i>number</i>;   snmp-command <i>command</i>;   source-port <i>port-number</i>;   ttl-threshold <i>number</i>;   uuid <i>hex-value</i>; }</pre>
Hierarchy Level	[edit <a href="#">applications</a> ], [edit <a href="#">applications application-set</a> <i>application-set-name</i> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure properties of an application and whether to include it in an application set.
Options	<p><b><i>application-name</i></b>—Identifier of the application.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">ALG Descriptions on page 126</a></li><li>• <a href="#">Configuring Application Sets on page 163</a></li><li>• <a href="#">Configuring Application Protocol Properties on page 146</a></li><li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li><li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li></ul>

## application-protocol

<b>Syntax</b>	<code>application-protocol <i>protocol-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications</a> <a href="#">application</a> <i>application-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>login</b> options introduced in Junos OS Release 7.4. <b>ip</b> option introduced in Junos OS Release 8.2.
<b>Description</b>	Identify the application protocol name. Application protocols are also called application layer gateways (ALGs).
<b>Options</b>	<p><b><i>protocol-name</i></b>—Name of the protocol. The following protocols are supported:</p> <ul style="list-style-type: none"> <li><b>bootp</b>—Bootstrap protocol</li> <li><b>dce-rpc</b>—DCE RPC</li> <li><b>dce-rpc-portmap</b>—DCE RPC portmap</li> <li><b>dns</b>—Domain Name Service</li> <li><b>exec</b>—Remote Execution Protocol</li> <li><b>ftp</b>—File Transfer Protocol</li> <li><b>h323</b>—H.323</li> <li><b>icmp</b>—ICMP</li> <li><b>iiop</b>—Internet Inter-ORB Protocol</li> <li><b>ip</b>—IP</li> <li><b>login</b>—Login</li> <li><b>netbios</b>—NetBIOS</li> <li><b>netshow</b>—NetShow</li> <li><b>pptp</b>—Point-to-Point Tunneling Protocol</li> <li><b>realaudio</b>—RealAudio</li> <li><b>rpc</b>—RPC</li> <li><b>rpc-portmap</b>—RPC portmap</li> <li><b>rtsp</b>—Real Time Streaming Protocol</li> <li><b>shell</b>—Shell</li> <li><b>sip</b>—Session Initiation Protocol</li> <li><b>snmp</b>—SNMP</li> <li><b>sqlnet</b>—SQLNet</li> <li><b>talk</b>—Talk Program</li> </ul>

**tftp**—Trivial File Transfer Protocol

**traceroute**—Traceroute

**winframe**—WinFrame

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [ALG Descriptions on page 126](#)
- [Configuring Application Sets on page 163](#)
- [Configuring Application Protocol Properties on page 146](#)
- [Examples: Configuring Application Protocols on page 177](#)
- [Verifying the Output of ALG Sessions on page 164](#)

---

## application-set

---

**Syntax** `application-set application-set-name {  
    application application-name;  
}`

**Hierarchy Level** [edit [applications](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure one or more applications to include in an application set.

**Options** *application-set-name*—Identifier of an application set.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [ALG Descriptions on page 126](#)
- [Configuring Application Sets on page 163](#)
- [Configuring Application Protocol Properties on page 146](#)
- [Examples: Configuring Application Protocols on page 177](#)
- [Verifying the Output of ALG Sessions on page 164](#)

## applications

---

<b>Syntax</b>	applications { ... }
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the applications used in services.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">ALG Descriptions on page 126</a></li><li>• <a href="#">Configuring Application Sets on page 163</a></li><li>• <a href="#">Configuring Application Protocol Properties on page 146</a></li><li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li><li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li></ul>

## destination-port

---

<b>Syntax</b>	<code>destination-port <i>port-value</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) destination port number.
<b>Options</b>	<b><i>port-value</i></b> —Identifier for the port or range of ports. For a complete list of supported application destination port requirements, see <a href="#">“Configuring Source and Destination Ports” on page 152</a> . <b>Range:</b> 1 through 65,535



**NOTE:** If you specify a value of 0 as a destination port or beginning of a destination report range, you will receive the following error:

```
'application application-name'  
  TCP Destination Port 0 Invalid  
error: configuration check-out failed
```

---

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">ALG Descriptions on page 126</a></li><li>• <a href="#">Configuring Application Sets on page 163</a></li><li>• <a href="#">Configuring Application Protocol Properties on page 146</a></li><li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li><li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li></ul>

## icmp-code

---

<b>Syntax</b>	<code>icmp-code value;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Internet Control Message Protocol (ICMP) code value.
<b>Options</b>	<b>value</b> —The ICMP code value. For a complete list, see “ <a href="#">Configuring the ICMP Code and Type</a> ” on page 150.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">ALG Descriptions on page 126</a></li> <li>• <a href="#">Configuring Application Sets on page 163</a></li> <li>• <a href="#">Configuring the ICMP Code and Type on page 150</a></li> <li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li> <li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li> </ul>

## icmp-type

---

<b>Syntax</b>	<code>icmp-type value;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	ICMP packet type value.
<b>Options</b>	<b>value</b> —The ICMP type value, such as <b>echo</b> or <b>echo-reply</b> . For a complete list, see “ <a href="#">Configuring the ICMP Code and Type</a> ” on page 150.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">ALG Descriptions on page 126</a></li> <li>• <a href="#">Configuring Application Sets on page 163</a></li> <li>• <a href="#">Configuring the ICMP Code and Type on page 150</a></li> <li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li> <li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li> </ul>

## inactivity-timeout

---

<b>Syntax</b>	<code>inactivity-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Inactivity timeout period, in seconds.
<b>Options</b>	<b><i>seconds</i></b> —Length of time the application is inactive before it times out. <b>Default:</b> 30 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">ALG Descriptions on page 126</a></li><li>• <a href="#">Configuring Application Sets on page 163</a></li><li>• <a href="#">Configuring the Inactivity Timeout Period on page 155</a></li><li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li><li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li></ul>

## learn-sip-register

---

<b>Syntax</b>	<code>learn-sip-register;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Activate SIP register to accept potential incoming SIP calls.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">ALG Descriptions on page 126</a></li><li>• <a href="#">Configuring Application Sets on page 163</a></li><li>• <a href="#">Configuring SIP on page 146</a></li><li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li><li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li></ul>

## protocol

<b>Syntax</b>	<code>protocol type;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Networking protocol type or number.
<b>Options</b>	<p><b>type</b>—Networking protocol type. The following text values are supported:</p> <ul style="list-style-type: none"> <li>ah</li> <li>egp</li> <li>esp</li> <li>gre</li> <li>icmp</li> <li>icmp6</li> <li>igmp</li> <li>ipip</li> <li>ospf</li> <li>pim</li> <li>rsvp</li> <li>tcp</li> <li>udp</li> </ul>



**NOTE:** IP version 6 (IPv6) is not supported as a network protocol in application definitions.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">ALG Descriptions on page 126</a></li> <li>• <a href="#">Configuring Application Sets on page 163</a></li> <li>• <a href="#">Configuring Application Protocol Properties on page 146</a></li> <li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li> <li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li> </ul>

## rpc-program-number

---

<b>Syntax</b>	<code>rpc-program-number <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Remote procedure call (RPC) or Distributed Computing Environment (DCE) value.
<b>Options</b>	<b><i>number</i></b> —RPC or DCE program value. <b>Range:</b> 100,000 through 400,000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">ALG Descriptions on page 126</a></li><li>• <a href="#">Configuring an RPC Program Number on page 163</a></li><li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li><li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li></ul>

## sip-call-hold-timeout

---

<b>Syntax</b>	<code>sip-call-hold-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Timeout period for SIP calls placed on hold, in seconds.
<b>Options</b>	<b><i>seconds</i></b> —Length of time the application holds a SIP call open before it times out. <b>Default:</b> 7200 seconds <b>Range:</b> 0 through 36,000 seconds (10 hours)
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">ALG Descriptions on page 126</a></li><li>• <a href="#">Configuring SIP on page 146</a></li><li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li><li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li></ul>

## snmp-command

---

<b>Syntax</b>	<code>snmp-command <i>command</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	SNMP command format.
<b>Options</b>	<i>command</i> —Supported commands are SNMP <a href="#">get</a> , <a href="#">get-next</a> , <a href="#">set</a> , and <a href="#">trap</a> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">ALG Descriptions on page 126</a></li> <li>• <a href="#">Configuring an SNMP Command for Packet Matching on page 162</a></li> <li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li> <li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li> </ul>

## source-port

---

<b>Syntax</b>	<code>source-port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Source port identifier.
<b>Options</b>	<i>port-value</i> —Identifier for the port. For a complete list, see “ <a href="#">Configuring Source and Destination Ports</a> ” on page 152.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">ALG Descriptions on page 126</a></li> <li>• <a href="#">Configuring Application Protocol Properties on page 146</a></li> <li>• <a href="#">Configuring Source and Destination Ports on page 152</a></li> <li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li> </ul>

## ttl-threshold

---

<b>Syntax</b>	<code>ttl-threshold <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the traceroute time-to-live (TTL) threshold value. This value sets the acceptable level of network penetration for trace routing.
<b>Options</b>	<i>number</i> —TTL threshold value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">ALG Descriptions on page 126</a></li><li>• <a href="#">Configuring the TTL Threshold on page 163</a>.</li><li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li><li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li></ul>

## uuid

---

<b>Syntax</b>	<code>uuid <i>hex-value</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">applications application application-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the Universal Unique Identifier (UUID) for DCE RPC objects.
<b>Options</b>	<i>hex-value</i> —Hexadecimal value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">ALG Descriptions on page 126</a></li><li>• <a href="#">Configuring a Universal Unique Identifier on page 163</a></li><li>• <a href="#">Examples: Configuring Application Protocols on page 177</a></li><li>• <a href="#">Verifying the Output of ALG Sessions on page 164</a></li></ul>

## CHAPTER 6

# Network Address Translation Configuration Guidelines

- [Network Address Translation Configuration Overview on page 191](#)
- [NAT Configuration Tasks on page 211](#)
- [Example: NAT 44 CGN Configurations on page 259](#)
- [Example: NATPT Configuration for the MS-MPC on page 263](#)
- [Example: Configuring NAT-PT on page 267](#)
- [Example: Configuring Inline Network Address Translation - Interface-Service Service Set on page 282](#)
- [Port Control Protocol Configuration Examples on page 290](#)
- [Carrier-Grade NAT Implementation: Best Practices on page 296](#)

## Network Address Translation Configuration Overview

---

- [Configuring Source and Destination Addresses Network Address Translation Overview on page 191](#)
- [Configuring Pools of Addresses and Ports for Network Address Translation Overview on page 192](#)
- [Configuring Address Pools for Network Address Port Translation \(NAPT\) Overview on page 194](#)
- [Network Address Translation Rules Overview on page 204](#)
- [Configuring Service Sets for Network Address Translation on page 209](#)

## Configuring Source and Destination Addresses Network Address Translation Overview

You must configure a specific address, a prefix, or the address-range boundaries:

- The following addresses, while valid in **inet.0**, cannot be used for NAT translation:
  - **0.0.0.0/32**
  - **127.0.0.0/8** (loopback)
  - **128.0.0.0/16** (martian)
  - **191.255.0.0/16** (martian)

- 192.0.0.0/24 (martian)
- 223.255.255.0/24 (martian)
- 224.0.0.0/4 (multicast)
- 240.0.0.0/4 (reserved)
- 255.255.255.255 (broadcast)
- You can specify one or more IPv4 address prefixes in the **pool** statement and in the **from** clause of the NAT rule term. This enables you to configure source translation from a private subnet to a public subnet without defining a rule term for each address in the subnet. Destination translation cannot be configured by this method. For more information, see *Examples: Configuring NAT Rules*.
- When you configure static source NAT, the **address** prefix size you configure at the **[edit services nat pool pool-name]** hierarchy level must be larger than the **source-address** prefix range configured at the **[edit services nat rule rule-name term term-name from]** hierarchy level. The **source-address** prefix range must also map to a single subnet or range of IPv4 or IPv6 addresses in the **pool** statement. Any pool addresses that are not used by the **source-address** prefix range are left unused. Pools cannot be shared.



**NOTE:** When you include a NAT configuration that changes IP addresses, it might affect forwarding path features elsewhere in your router configuration, such as source class usage (SCU), destination class usage (DCU), filter-based forwarding, or other features that target specific IP addresses or prefixes.

NAT configuration might also affect routing protocol operation, because the protocol peering, neighbor, and interface addresses can be altered when routing protocols packets transit the Adaptive Services (AS) or Multiservices PIC.

## Configuring Pools of Addresses and Ports for Network Address Translation Overview

- [Configuring NAT Pools on page 192](#)
- [Preserve Range and Preserve Parity on page 193](#)
- [Specifying Destination and Source Prefixes without Configuring a Pool on page 194](#)

### Configuring NAT Pools

You can use the **pool** statement to define the addresses (or prefixes), address ranges, and ports used for Network Address Translation (NAT). To configure the information, include the **pool** statement at the **[edit services nat]** hierarchy level:

```
[edit services nat]
pool nat-pool-name {
  address ip-prefix</prefix-length>;
  address-range low minimum-value high maximum-value;
  port (automatic | range low minimum-value high maximum-value);
  preserve-parity;
  preserve-range {
```

```
}
}
```

To configure pools for traditional NAT, specify either a destination pool or a source pool.

With static source NAT and dynamic source NAT, you can specify multiple IPv4 addresses (or prefixes) and IPv4 address ranges. Up to 32 prefixes or address ranges (or a combination) can be supported within a single pool.

With static destination NAT, you can also specify multiple address prefixes and address ranges in a single term. Multiple destination NAT terms can share a destination NAT pool. However, the netmask or range for the **from** address must be smaller than or equal to the netmask or range for the destination pool address. If you define the pool to be larger than required, some addresses will not be used. For example, if you define the pool size as 100 addresses and the rule specifies only 80 addresses, the last 20 addresses in the pool are not used.

For constraints on specific translation types, see [“Network Address Translation Rules Overview” on page 204](#).

With source static NAT, the prefixes and address ranges cannot overlap between separate pools.

In an address range, the **low** value must be a lower number than the **high** value. When multiple address ranges and prefixes are configured, the prefixes are depleted first, followed by the address ranges.

When you specify a port for dynamic source NAT, address ranges are limited to a maximum of 65,000 addresses, for a total of (65,000 x 65,535) or 4,259,775,000 flows. A dynamic NAT pool with no address port translation supports up to 65,535 addresses. There is no limit on the pool size for static source NAT.

### Preserve Range and Preserve Parity

You can configure your carrier-grade NAT (CGN) to preserve the range or parity of the packet source port when it allocates a source port for an outbound connection. You can configure the preserve parity and preserve range options under the NAT pool definition by including the **preserve-range** and **preserve-parity** configuration statements at the **[edit services nat pool poolname port]** hierarchy level.

- **Preserve range**—RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*, defines two ranges: 0 through 1023, and 1024 through 65,535. When the **preserve-range** knob is configured and the incoming port falls into one of these ranges, CGN allocates a port from that range only. However, if there is no available port in the range, the port allocation request fails and that session is not created. The failure is reflected on counters and system logging, but no Internet Control Message Protocol (ICMP) message is generated. If this knob is not configured, allocation is based on the configured port range without regard to the port range that contains the incoming port. The exception is some application-level gateways (ALGs), such as hello, that have special zones.
- **Preserve parity**—When the **preserve-parity** knob is configured, CGN allocates a port with the same even or odd parity as the incoming port. If the incoming port number is

odd or even, the outgoing port number should correspondingly be odd or even. If a port number of the desired parity is not available, the port allocation request fails, the session is not created, and the packet is dropped.

### Specifying Destination and Source Prefixes without Configuring a Pool

You can directly specify the destination or source prefix used in NAT without configuring a pool.

To configure the information, include the **rule** statement at the **[edit services nat]** hierarchy level:

```
[edit services nat]
rule rule-name {
  term term-name {
    then {
      translated {
        destination-prefix prefix;
      }
    }
  }
}
```

## Configuring Address Pools for Network Address Port Translation (NAPT) Overview

With Network Address Port Translation (NAPT), you can configure up to 32 address ranges with up to 65,536 addresses each.

The **port** statement specifies port assignment for the translated addresses. To configure automatic assignment of ports, include the **port automatic** statement at the **[edit services nat pool nat-pool-name]** hierarchy level. To configure a specific range of port numbers, include the **port range low minimum-value high maximum-value** statement at the **[edit services nat pool nat-pool-name]** hierarchy level.



**NOTE:** When 99% of the total available ports in pool for napt-44 , no new flows are allowed on that NAT pool.

---

The Junos OS provides several alternatives for allocating ports:

- [Round-Robin Allocation for NAPT on page 195](#)
- [Sequential Allocation for NAPT on page 195](#)
- [Preserve Parity and Preserve Range for NAPT on page 196](#)
- [Address Pooling and Endpoint Independent Mapping for NAPT on page 196](#)
- [Port Block Allocation for NAPT on page 198](#)
- [Deterministic Port Block Allocation for NAPT on page 199](#)
- [Comparision of NAPT Implementation Methods on page 203](#)

### Round-Robin Allocation for NAPT

To configure round-robin allocation for NAT pools, include the **address-allocation round-robin** configuration statement at the **[edit services nat pool *pool-name*]** hierarchy level. When you use round-robin allocation, one port is allocated from each address in a range before repeating the process for each address in the next range. After ports have been allocated for all addresses in the last range, the allocation process wraps around and allocates the next unused port for addresses in the first range.

- The first connection is allocated to the address:port 100.0.0.1:3333.
- The second connection is allocated to the address:port 100.0.0.2:3333.
- The third connection is allocated to the address:port 100.0.0.3:3333.
- The fourth connection is allocated to the address:port 100.0.0.4:3333.
- The fifth connection is allocated to the address:port 100.0.0.5:3333.
- The sixth connection is allocated to the address:port 100.0.0.6:3333.
- The seventh connection is allocated to the address:port 100.0.0.7:3333.
- The eighth connection is allocated to the address:port 100.0.0.8:3333.
- The ninth connection is allocated to the address:port 100.0.0.9:3333.
- The tenth connection is allocated to the address:port 100.0.0.10:3333.
- The eleventh connection is allocated to the address:port 100.0.0.11:3333.
- The twelfth connection is allocated to the address:port 100.0.0.12:3333.
- Wraparound occurs and the thirteenth connection is allocated to the address:port 100.0.0.1:3334.

### Sequential Allocation for NAPT

With sequential allocation, the next available address in the NAT pool is selected only when all the ports available from an address are exhausted.



**NOTE:** This legacy implementation provides backward compatibility and is no longer a recommended approach..

The NAT pool called **napt** in the following configuration example uses the sequential implementation:

```
pool napt {
  address-range low 100.0.0.1 high 100.0.0.3;
  address-range low 100.0.0.4 high 100.0.0.6;
  address-range low 100.0.0.8 high 100.0.0.10;
  address-range low 100.0.0.12 high 100.0.0.13;
  port {
    range low 3333 high 3334;
  }
}
```

```
}
```

In this example, the ports are allocated starting from the first address in the first address-range, and allocation continues from this address until all available ports have been used. When all available ports have been used, the next address (in the same address-range or in the following address-range) is allocated and all its ports are selected as needed. In the case of the example **napt** pool, the tuple address, port 100.0.0.4:3333, is allocated only when all ports for all the addresses in the first range have been used.

- The first connection is allocated to the address:port 100.0.0.1:3333.
- The second connection is allocated to the address:port 100.0.0.1:3334.
- The third connection is allocated to the address:port 100.0.0.2:3333.
- The fourth connection is allocated to the address:port 100.0.0.2:3334, and so on.

---

### Preserve Parity and Preserve Range for NAPT

The following options are available for NAPT:

- Preserving parity—Use the **preserve-parity** command to allocate even ports for packets with even source ports and odd ports for packets with odd source ports.
- Preserving range—Use the **preserve-range** command to allocate ports within a range from 0 to 1023, assuming the original packet contains a source port in the reserved range. This applies to control sessions, not data sessions.

---

### Address Pooling and Endpoint Independent Mapping for NAPT

- [Address Pooling and Endpoint Independent Mapping for NAPT on page 196](#)

#### *Address Pooling and Endpoint Independent Mapping for NAPT*

##### *Address Pooling*

Address pooling, or address pooling paired (APP) ensures assignment of the same external IP address for all sessions originating from the same internal host. You can use this feature when assigning external IP addresses from a pool. This option does not affect port utilization

Address pooling solves the problems of an application opening multiple connections. For example, when Session Initiation Protocol (SIP) client sends Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) packets, the SIP generally server requires that they come from the same IP address, even if they have been subject to NAT. If RTP and RTCP IP addresses are different, the receiving endpoint might drop packets. Any point-to-point (P2P) protocol that negotiates ports (assuming address stability) benefits from address pooling paired.

The following are use cases for address pooling.

- A site that offers instant messaging services requires that chat and their control sessions come from the same public source address. When the user signs on to chat, a control session authenticates the user. A different session begins when the user starts a chat session. If the chat session originates from a source address that is different from the

authentication session, the instant messaging server rejects the chat session, because it originates from an unauthorized address.

- Certain websites such as online banking sites require that all connections from a given host come from the same IP address.



**NOTE:** Starting with Junos OS Release 14.1, when you deactivate a service-set that contains address pooling paired (APP) for that service-set, messages are displayed on the PIC console and the mappings are cleared for that service-set. These messages are triggered when the deletion of a service-set commences and again generated when the deletion of the service-set is completed. The following sample messages are displayed when deletion starts and ends:

- Nov 15 08:33:13.974 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion initiated
- Nov 15 08:33:14.674 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion completed

In a scaled environment that contains a large number of APP in a service set, a heavy volume of messages is generated and this process takes some amount of time. We recommend that you wait until the console messages indicating the completion of deletion of the service set are completed before you reactivate the service-set again.

---

### ***Endpoint Independent Mapping and Endpoint Independent Filtering***

Endpoint independent mapping (EIM) ensures the assignment of the same external address *and* port for all connections from a given host if they use the same internal port. This means if they come from a different source port, you are free to assign a different external address.

EIM and APP differ as follows:

- APP ensures assigning the same external IP address.
- EIM provides a stable external IP address and port (for a period of time) to which external hosts can connect. Endpoint independent filtering (EIF) controls which external hosts can connect to an internal host.



**NOTE:** Starting with Junos OS Release 14.1, when you deactivate a service-set that contains endpoint independent mapping (EIM) mapping for that service-set, messages are displayed on the PIC console and the mappings are cleared for that service-set. These messages are triggered when the deletion of a service-set commences and again generated when the deletion of the service-set is completed. The following sample messages are displayed when deletion starts and ends:

- Nov 15 08:33:13.974 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion initiated
- Nov 15 08:33:14.674 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion completed

In a scaled environment that contains a large number of EIM mappings in a service set, a heavy volume of messages is generated and this process takes some amount of time. We recommend that you wait until the console messages indicating the completion of deletion of the service set are completed before you reactivate the service-set again.

---

### Port Block Allocation for NAPT

Carriers track subscribers using the IP address (RADIUS or DHCP) log. If they use NAPT, an IP address is shared by multiple subscribers, and the carrier must track the IP address and port, which are part of the NAT log. Because ports are used and reused at a very high rate, tracking subscribers using the log becomes difficult due to the large number of messages, which are difficult to archive and correlate. By enabling the allocation of ports in blocks, port block allocation can significantly reduce the number of logs, making it easier to track subscribers.

Port block allocation is supported on MX series routers with MultiServices Dense Port Concentrators (MS-DPCs).

- [Secured Port Block Allocation for NAPT on page 198](#)
- [Interim Logging for Port Block Allocation on page 199](#)

#### ***Secured Port Block Allocation for NAPT***

Secured port block allocation can be used for translation types **napt-44** and **stateful-nat64**.

When allocating blocks of ports, the most recently allocated block is the current active block. New requests for NAT ports are served from the active block. Ports are allocated randomly from the current active block.

When you configure secured port block allocation, you can specify the following:

- **block-size**
- **max-blocks-per-address**
- **active-block-timeout**

### *Interim Logging for Port Block Allocation*

With port block allocation we generate one syslog log per set of ports allocated for a subscriber. These logs are UDP based and can be lost in the network, particularly for long-running flows. Interim logging triggers re-sending the above logs at a configured interval for active blocks that have traffic on at least one of the ports of the block.

Interim logging is activated by including the **pba-interim-logging-interval** statement under **services-options** for sp- interfaces.

### **Deterministic Port Block Allocation for NAT**

You can configure NAT algorithm-based allocation of blocks of destination ports. By specifying **deterministic-port-block-allocation blocksize blocksize** at the **[edit services nat pool poolname port]** hierarchy level, you ensure that an incoming (source) IP address and port always map to the same destination IP address and port, thus eliminating the need for the address translation logging. You can also specify **include-boundary-addresses** if you want the lowest and highest addresses in the source address range of a NAT rule to be translated when the NAT pool is used. When you use deterministic port block allocation, you must specify **deterministic-nat44** as the **translation-type** in your NAT rule.

For detailed information on how to configure deterministic port block allocation, see [“Configuring Deterministic Port Block Allocation” on page 237](#).

- [Understanding Deterministic Port Block Allocation Algorithms on page 199](#)
- [Deterministic Port Block Allocation Algorithm Usage on page 200](#)
- [Deterministic Port Block Allocation Restrictions on page 202](#)

### **Understanding Deterministic Port Block Allocation Algorithms**

The effectiveness of your implementation of deterministic port block allocation depends on your analysis of your subscriber requirements. The block size you provide indicates how many ports will be made available for each incoming subscriber address in the range the **from** clause specified in the applicable NAT rule. The allocation algorithm computes an offset value to determine the outgoing port. A reverse algorithm is used to derive the originating subscriber address.



**NOTE:** In order to track subscribers without using logs, an ISP must use a reverse algorithm to derive a subscriber (source) addresses from translated addresses.

***Deterministic Port Block Allocation Algorithm Usage***

When you have configured deterministic port block allocation, you can use the ***show services nat deterministic-nat internal-host*** and ***show services nat deterministic-nat nat-port-block*** commands to show forward and reverse mapping. However, mappings will change if you reconfigure your deterministic port block allocation block size or the **from** clause for your NAT rule. In order to provide historical information on mappings, we recommend that you write scripts that can show specific mappings for prior configurations.

The following variables are used in forward calculation (private subscriber IP address to public IP address) and reverse calculation (public IP address to private subscriber IP address):

- Pr\_Prefix—Any pre-NAT IPv4 subscriber address
- Pr\_Port—Any pre-NAT protocol port
- Block\_Size—Number of ports configured to be available for each Pr\_Prefix
- Base\_PR\_Prefix—First usable pre-NAT IPv4 subscriber address in a “from” clause match condition
- Base\_PU\_Prefix—First usable post-NAT IPv4 subscriber address configured in the NAT pool.
- Pu\_Port\_Range\_Start—1024 (ports 0 through 1023 are not used when **port automatic** is configured)
- Pr\_Offset—Pr\_Prefix – Base\_Pr\_Prefix
- PR\_Port\_Offset—Pr\_Offset \* Block\_Size
- Pu\_Prefix—Post-NAT address for a given Pr\_Prefix
- Pu\_Start\_Port—Post-NAT start port for a flow from a given Pr\_Prefix
- Pu\_Actual\_Port—Post-NAT port seen on a reverse flow
- Nr\_Addr\_PR\_Prefix — Number of usable pre-NAT IPv4 subscriber addresses in a “from” clause match condition
- Nr\_Addr\_PU\_Prefix — Number of usable post-NAT IPv4 addresses configured in the NAT pool
- Rounded\_Port\_Range\_Per\_IP —  $\text{ceil}[(\text{Nr\_Addr\_PR\_Prefix}/\text{Nr\_Addr\_PU\_Prefix})] * \text{Block\_Size}$
- Pu\_Offset—Pu\_Prefix – Base\_Pu\_Prefix
- Pu\_Port\_Offset— $(\text{Pu\_Offset} * \text{Port\_Range\_Per\_Pu\_IP}) + (\text{Pu\_Actual\_Port} - \text{Pu\_Port\_Start\_Port})$



**NOTE:** If `block-size` is configured as zero, the method for computing the block size has changed and is computed as follows:

$$\text{block-size} = \text{int}(\text{ceil}[(\text{Nr\_Addr\_PR\_Prefix} / \text{Nr\_Addr\_PU\_Prefix})])$$

where 64512 is the maximum available port range per public IP address.

**Algorithm Usage**—Assume the following configuration:

```
services {
  nat {
    pool src-pool {
      address-range low 32.32.32.1 high 32.32.32.254;
      port {
        automatic {
          random-allocation;
        }
        deterministic-block-allocation {
          block-size 249;
        }
      }
    }
  }
  rule det-nat {
    match-direction input;
    term t1 {
      from {
        source-address {
          10.1.0.0/16;
        }
      }
      then {
        translated {
          source-pool src-pool;
          translation-type {
            deterministic-napt44;
          }
        }
      }
    }
  }
}
```

#### Forward Translation

1.  $\text{Pr\_Offset} = \text{Pr\_Prefix} - \text{Base\_Pr\_Prefix}$
2.  $\text{Pr\_Port\_Offset} = \text{Pr\_Offset} * \text{Block\_Size}$
3.  $\text{Rounded\_Port\_Range\_Per\_IP} = \text{ceil}[(\text{Nr\_Addr\_PR\_Prefix} / \text{Nr\_Addr\_PU\_Prefix})] * \text{Block\_Size}$
4.  $\text{Pu\_Prefix} = \text{Base\_Public\_Prefix} + \text{floor}(\text{Pr\_Port\_Offset} / \text{Rounded\_Port\_Range\_Per\_IP})$
5.  $\text{Pu\_Start\_Port} = \text{Pu\_Port\_Range\_Start} + (\text{Pr\_Port\_Offset} \% \text{Rounded\_Port\_Range\_Per\_IP})$

Using the sample configuration and assuming a subscriber flow sourced from 10.1.1.250:5000:

1.  $Pr\_Offset = 10.1.1.250 - 10.1.0.1 = 505$
2.  $Pu\_Port\_Offset = 505 * 249 = 125,745$
3.  $Rounded\_Port\_Range\_Per\_IP = \text{ceil}[(65, 533/254)] * 249 = 259 * 249 = 64,491$
4.  $Pu\_Prefix = 32.32.32.1 + \text{floor}(125,745 / 64,491) = 32.32.32.1 + 1 = 32.32.32.2$
5.  $Pu\_Start\_Port = 1,024 + (125,745 \% 64,491) = 62278$ 
  - 10.1.1.250 is translated to 32.32.32.2.
  - The starting port is 62278. There are 249 ports available to the subscriber based on the configured block size. The available port range spans ports 62278 through 62526 (inclusive).
  - The specific flow 10.1.1.250:5000 randomly assigns any of the ports in its range because random allocation was specified.

#### Reverse Translation

1.  $Pu\_Offset = Pu\_Prefix - Base\_Pu\_Prefix$
2.  $Pu\_Port\_Offset = (Pu\_Offset * Rounded\_Port\_Range\_Per\_IP) + (Pu\_Actual\_Port - Pu\_Port\_Range\_Start)$
3.  $Subscriber\_IP = Base\_Pr\_Prefix + \text{floor}(Pu\_Port\_Offset / Block\_Size)$

The reverse translation is determined as follows. Assume a flow returning to 32.32.32.2:62278.

1.  $Pu\_Offset = 32.32.32.2 - 32.32.32.1 = 1$
2.  $Pu\_Port\_Offset = (1 * 64,491) + (62,280 - 1024) = 125,747$
3.  $Subscriber\_IP = 10.1.0.1 + \text{floor}(125,747 / 249) = 10.1.0.1 + 505 = 10.1.1.250$



**NOTE:** In reverse translation, only the original private IP address can be derived, and not the original port in use. This is sufficiently granular for law enforcement requirements.

---

#### *Deterministic Port Block Allocation Restrictions*

When you configure deterministic port block allocation, you must be aware of the following restrictions. Violation of any restriction results in a commit error. The restrictions and their error messages are shown in [Table 24 on page 203](#)

Table 24: Deterministic Port Block Allocation Commit Constraints

Restriction	Error Message
The total number of deterministic NAT blocks must be greater than or equal to the 'from' clause addresses configured. This means that the Rounded_Port_Range_Per_IP value must be less than or equal to 64,512.	Number of addresses and port blocks combination in the NAT pool is less than number of addresses in 'from' clause
IPv6 addresses should not be used in deterministic NAT pool/from clause.	Invalid IP address in pool p1 with translation type deterministic-napt44  OR  There is already a range configured with v4 address range
The <b>from</b> clause addresses should be same if the same deterministic NAT pool is used across multiple terms/rules. Only one <b>from</b> clause address/range should be specified if the same deterministic NAT pool is used across multiple terms/rules.	With translation-type deterministic-napt44, same 'from' address/range should be configured if pool is shared by multiple rules or terms
There shouldn't be address overlap between <b>except</b> entries in the <b>from</b> clause addresses.	overlapping address, in the 'from' clause between 'except' entries
A deterministic NAT pool cannot be used with other translation-types	Deterministic NAT pool cannot be used with other translation-types
Deterministic NAPT44 must use a source pool with deterministic-port-block-allocation configuration	Deterministic NAPT44 must use a source pool with deterministic-port-block-allocation configuration
If <b>address-allocation round-robin</b> is configured, a commit results in display of a warning indicating that this technique is not needed with translation-type deterministic-napt44 and is ignored.	Address allocation round-robin is not needed with translation-type deterministic-napt44
The total number of IP addresses assigned to a deterministic NAT pool should be less than or equal to $2^{24}$ (16777216).	Number of addresses in pool with deterministic-napt44 translation are limited to at most 16777216 ( $2^{24}$ )

### Comparison of NAPT Implementation Methods

Table 25 on page 203 provides a feature comparison of available NAPT implementation methods.

Table 25: Comparison of NAPT Implementation Methods

Feature/Function	Dynamic Port Allocation	Secured Port Block Allocation	Deterministic Port Block Allocation
Users per IP	High	Medium	Low
Security Risk	Low	Medium	Medium
Log Utilization	High	Low	None (no logs necessary)
Security Risk Reduction	Random allocation	<b>active-block-timeout</b> feature	n/a

Table 25: Comparison of NAT Implementation Methods (*continued*)

Feature/Function	Dynamic Port Allocation	Secured Port Block Allocation	Deterministic Port Block Allocation
Increasing Users per IP	n/a	Configure multiples of smaller port blocks to maximize users/ public IP	Algorithm-based port allocation

## Network Address Translation Rules Overview

To configure a NAT rule, include the **rule** *rule-name* statement at the **[edit services nat]** hierarchy level:

```
[edit services nat]
rule rule-name {
  match-direction (input | output);
  term term-name {
    from (Services NAT) {
      application-sets (Services NAT) set-name;
      applications (Services NAT) [ application-names ];
      destination-address (address | any-unicast) <except>;
      destination-address-range low minimum-value high maximum-value <except>;
      destination-prefix-list list-name <except>;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
      source-prefix-list list-name <except>;
    }
    then {
      no-translation;
      translated {
        address-pooling paired;
        destination-pool nat-pool-name;
        destination-prefix destination-prefix;
        dns-alg-pool dns-alg-pool;
        dns-alg-prefix dns-alg-prefix;
        filtering-type endpoint-independent;
        mapping-type endpoint-independent;
        overload-pool overload-pool-name;
        overload-prefix overload-prefix;
        source-pool nat-pool-name;
        source-prefix source-prefix;
        translation-type {
          (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | dynamic-nat44 | napt-44 |
            napt-66 | napt-pt | stateful-nat64 | twice-basic-nat-44 | twice-dynamic-nat-44
            | twice-napt-44);
        }
      }
    }
    syslog;
  }
}
```

Each rule must include a **match-direction** statement that specifies the direction in which the match is applied.

In addition, each NAT rule consists of a set of terms, similar to a firewall filter. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software.

The following sections explain how the components of NAT rules:

- [Configuring Match Direction for NAT Rules on page 205](#)
- [Configuring Match Conditions in NAT Rules on page 205](#)
- [Configuring Actions in NAT Rules on page 206](#)
- [Configuring Translation Types on page 207](#)

### Configuring Match Direction for NAT Rules

Each rule must include a **match-direction** statement that specifies the direction in which the match is applied. To configure where the match is applied, include the **match-direction** statement at the **[edit services nat rule rule-name]** hierarchy level:

```
[edit services nat rule rule-name]
match-direction (input | output);
```

The match direction is used with respect to the traffic flow through the Multiservices DPC and Multiservices PICs. When a packet is sent to the PIC, direction information is carried along with it. The packet direction is determined based on the following criteria:

- With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.
- With a next-hop service set, packet direction is determined by the interface used to route the packet to the Multiservices DPC or Multiservices PIC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the PIC or DPC, the packet direction is output. For more information about inside and outside interfaces, see [“Configuring Service Sets to be Applied to Services Interfaces” on page 742.](#)
- On the Multiservices DPC and Multiservices PIC, a flow lookup is performed. If no flow is found, rule processing is performed. All rules in the service set are considered. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that matches the packet direction are considered.

### Configuring Match Conditions in NAT Rules

To configure NAT match conditions, include the **from** statement at the **[edit services nat rule rule-name term term-name]** hierarchy level:

```
[edit services nat rule rule-name term term-name]
from {
  application-sets set-name;
  applications [ application-names ];
```

```

destination-address (address | any-unicast) <except>;
destination-address-range low minimum-value high maximum-value <except>;
destination-prefix-list list-name <except>;
source-address (address | any-unicast) <except>;
source-address-range low minimum-value high maximum-value <except>;
source-prefix-list list-name <except>;
}

```

To configure traditional NAT, you can use the destination address, a range of destination addresses, the source address, or a range of source addresses as a match condition, in the same way that you would configure a firewall filter; for more information, see the *Routing Policy Feature Guide for Routing Devices*.

Alternatively, you can specify a list of source or destination prefixes by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either the **destination-prefix-list** or **source-prefix-list** statement in the NAT rule. For an example, see [“Examples: Configuring Stateful Firewall Rules” on page 392.](#)

If the **translation-type** statement in the **then** statement of the nat rule is set to **stateful-nat-64**, the range specified by the **destination-address-range** or the **destination-prefix-list** in the **from** statement must be within the range specified by the **destination-prefix** statement in the **then** statement.

### Configuring Actions in NAT Rules

To configure NAT actions, include the **then** statement at the **[edit services nat rule rule-name term term-name]** hierarchy level:

**Restriction for NAT rules with translation type stateful-nat-64**—In Junos OS Release 13.2 and earlier, the following restriction was not enforced by the CLI: if the **translation-type** statement in the **then** statement of a NAT rule was set to **stateful-nat-64**, the range specified by the **destination-address-range** or the **destination-prefix-list** in the **from** statement needed to be within the range specified by the **destination-prefix** statement in the **then** statement. Starting in Junos OS Release 13.3R1, this restriction is enforced.

```

[edit services nat]
rule rule-name {
  term term-name {
    from {
      destination-address-range low minimum-value high maximum-value <except>;
      destination-prefix-list list-name <except>;
    }
    then {
      destination-prefix destination-prefix;
    }
  }
}

```

```

[edit services nat rule rule-name term term-name]
then {
  no-translation;
  syslog;
  translated {
    destination-pool nat-pool-name;
    destination-prefix destination-prefix;
    source-pool nat-pool-name;
    source-prefix source-prefix;
  }
}

```

```

    translation-type (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | dynamic-nat44
    | napt-44 | napt-66 | napt-pt | stateful-nat64 | twice-basic-nat-44 |
    twice-dynamic-nat-44 | twice-napt-44);
  }
}

```

The **no-translation** statement allows you to specify addresses that you want excluded from NAT.

The **system log** statement enables you to record an alert in the system logging facility.

The **destination-pool**, **destination-prefix**, **source-pool**, and **source-prefix** statements specify addressing information that you define by including the **pool** statement at the **[edit services nat]** hierarchy level; for more information, see “[Configuring Pools of Addresses and Ports for Network Address Translation Overview](#)” on page 192.

### Configuring Translation Types

The **translation-type** statement specifies the type of NAT used for source or destination traffic. The options are **basic-nat-pt**, **basic-nat44**, **basic-nat66**, **dnat-44**, **dynamic-nat44**, **napt-44**, **napt-66**, **napt-pt**, **stateful-nat64**, **twice-basic-nat-44**, **twice-dynamic-nat-44**, and **twice-napt-44**.

The implementation details of the nine options of the **translation-type** statement are as follows:

- **basic-nat44**—This option implements the static translation of source IP addresses without port mapping. You must configure the **from source-address** statement in the match condition for the rule. The size of the address range specified in the statement must be the same as or smaller than the source pool. You must specify either a source pool or a destination prefix. The referenced pool can contain multiple addresses but you cannot specify ports for translation.



**NOTE:** In an interface service set, all packets destined for the source address specified in the match condition are automatically routed to the services PIC, even if no service set is associated with the interface.



**NOTE:** Prior to Junos OS Release 11.4R3, you could only use a source NAT pool in a single service set. As of Junos OS Release 11.4R3 and subsequent releases, you can reuse a source NAT pool in multiple service sets.

- **basic-nat66**—This option implements the static translation of source IP addresses without port mapping in IPv6 networks. The configuration is similar to the **basic-nat44** implementation, but with IPv6 addresses.
- **basic-nat-pt**—This option implements translation of addresses of IPv6 hosts, as they originate sessions to the IPv4 hosts in an external domain and vice versa. This option is always implemented with DNS ALG. You must define the source and destination pools of IPv4 addresses. You must configure one rule and define two terms. Configure

the IPv6 addresses in the **from** statement in both **term** statements. In the **then** statement of the first term within the rule, reference both the source and destination pools and configure **dns-alg-prefix**. Configure the source prefix in the **then** statement of the second term within the same rule.

- **dnat-44**—This option implements static translation of destination IP addresses without port mapping. The size of the pool address space must be greater than or equal to the destination address space. You must specify a name for the **destination pool** statement. The referenced pool can contain multiple addresses, ranges, or prefixes, as long as the number of NAT addresses in the pool is larger than the number of destination addresses in the **from** statement. You must include exactly one **destination-address** value at the **[edit services nat rule rule-name term term-name from]** hierarchy level; if it is a prefix, the size must be less than or equal to the pool prefix size. Any addresses in the pool that are not matched in the yvalue remain unused, because a pool cannot be shared among multiple terms or rules.
- **dynamic-nat44**—This option implements dynamic translation of source IP addresses without port mapping. You must specify a **source-pool**. The referenced pool must include an **address** configuration (for address-only translation).

The **dynamic-nat44** address-only option supports translating up to 16,777,216 addresses to a smaller size pool. The requests from the source address range are assigned to the addresses in the pool until the pool is used up, and any additional requests are rejected. A NAT address assigned to a host is used for all concurrent sessions from that host. The address is released to the pool only after all the sessions for that host expire. This feature enables the router to share a few public IP addresses between several private hosts. Because all the private hosts might not simultaneously create sessions, they can share a few public IP addresses.

- **napt-44**—This option implements dynamic translation of source IP addresses with port mapping. You must specify a name for the **source-pool** statement. The referenced pool must include a **port** configuration. If the port is configured as automatic or a port range is specified, then it implies that Network Address Port Translation (NAPT) is used.
- **napt-66**—This option implements dynamic address translation of source IP addresses with port mapping for IPv6 addresses. The configuration is similar to the **napt-44** implementation, but with IPv6 addresses.
- **napt-pt**—This option implements dynamic address and port translation for source and static translation of destination IP address. You must specify a name for the **source-pool** statement. The referenced pool must include a port configuration (for NAPT). Additionally, you must configure two rules, one for the DNS traffic and the other for the rest of the traffic. The rule meant for the DNS traffic should be DNS ALG enabled and the **dns-alg-prefix** statement should be configured. Moreover, the prefix configured in the **dns-alg-prefix** statement must be used in the second rule to translate the destination IPv6 addresses to IPv4 addresses.
- **stateful-nat64**—This option implements dynamic address and port translation for source IP addresses and prefix removal translation for destination IP addresses. You must specify the IPv4 addresses used for translation at the **[edit services nat pool]**

hierarchy level. This pool must be referenced in the rule that translates the IPv6 addresses to IPv4.

- **twice-basic-nat-44**—This option implements static source and static destination translation for IPv4 addresses, thus combining **basic-nat44** for source and **dnat-44** for destination addresses.
- **twice-dynamic-nat-44**—This option implements source dynamic and destination static translation for IPv4 addresses, combining **dynamic-nat44** for source and **dnat-44** for destination addresses.
- **twice-napt-44**—This option implements source NAPT and destination static translation for IPv4 addresses, combining **napt-44** for source and **dnat-44** for destination addresses.



**NOTE:** When configuring NAT, if any traffic is destined for the following addresses and does not match a NAT flow or NAT rule, the traffic is dropped:

- Addresses specified in the **from destination-address** statement when you are using destination translation
  - Addresses specified in the source NAT pool when you are using source translation
- 

For more information on NAT methods, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

## Configuring Service Sets for Network Address Translation

When configuring a service set for NAT processing, make sure you have defined:

- Service interface(s) for handling inbound and outbound traffic



**NOTE:** Prior to Junos OS Release 11.4R3, you could only use a source NAT pool in a single service set. As of Junos OS Release 11.4R3 and subsequent releases, you can reuse a source or destination NAT pool in multiple service sets, provided that the service interfaces associated with the service sets are in different virtual routing and forwarding (VRF) instances.

- For interface style service sets, when a NAT pool is reused in multiple service sets, the service interfaces used in the `interface-service` `service-interface` option of each service set must be in different VRFs.
- For next-hop style service sets, when a NAT pool is reused in multiple service sets, the service interfaces used in the `outside-interface` option of each service set must be in different VRFs.

*Not adhering to these service interface restrictions will cause multiple routes to be installed in the same VRF for the same NAT addresses, causing reverse traffic to be processed incorrectly.*

To enable sharing of source NAT pools, include the `allow-overlapping-nat-pools` statement at the `[edit services nat]` hierarchy level.

- 
- A NAT rule or ruleset



**NOTE:** To configure an MX-DPC interface to be used exclusively for carrier-grade NAT (CGN) or related services (intrusion detection, stateful firewall, and software), include the `cg-n-pic` statement at the `[edit interfaces interface-name services-options]` hierarchy level.

To configure a NAT service set:

1. At the `[edit services]` hierarchy level, define the service set.

```
[edit services]
user@host# edit service-set service-set-name
```

2. Configure either an interface service, which requires a single service interface, or a next-hop service, which requires an inside and outside service interface.

```
[edit services service-set service-set-name]
user@host# set interface-service service-interface interface-name
```

Or

```
[edit services service-set service-set-name]
user@host# set next-hop-service inside-service-interface interface-name
                        outside-service-interface interface-name
```



**NOTE:** If you have a Trio-based line card (MPC/MIC), you can use an inline-services interface that was configured on that card, as shown in this example:

```
[edit]
user@host# set interfaces si-0/0/0
[edit services service-set s1]
user@host# set interface-service service-interface si-0/0/0
```

For more information on interface service and next-hop service, see [“Configuring Service Sets to be Applied to Services Interfaces” on page 742.](#)

3. Configure a reference to the NAT rules or ruleset to be used with the service set.

```
[edit services service-set service-set-name]
user@host# set nat-rules rule-or-ruleset-name
```

4. (Optional) For NAT64, specify that the don't fragment (DF) bit for IPv4 packet headers is cleared when packet length is less than 1280 bytes.

```
[edit services service-set service-set-name]
user@host# set nat-options stateful-nat64 clear-dont-fragment-bit
```

## NAT Configuration Tasks

- [Configuring Static Source Translation in IPv4 Networks on page 212](#)
- [Configuring Static Source Translation in IPv6 Networks on page 217](#)
- [Configuring Static Destination Address Translation in IPv4 Networks on page 221](#)
- [Configuring Dynamic Address-Only Source Translation in IPv4 Networks on page 225](#)
- [Configuring Dynamic Source Address and Port Translation in IPv4 Networks on page 229](#)
- [Configuring Dynamic Source Address and Port Translation for IPv6 Networks on page 233](#)
- [Configuring Secured Port Block Allocation on page 235](#)
- [Configuring Deterministic Port Block Allocation on page 237](#)
- [Configuring Stateful NAT64 on page 238](#)
- [Configuring Protocol Translation Between IPv6 and IPv4 Networks - NAT-PT on page 240](#)
- [Example: Assigning Addresses from a Dynamic Pool for Static Use on page 246](#)
- [Example: Configuring NAT for Multicast Traffic on page 247](#)
- [Configuring Port Forwarding for Static Destination Address Translation on page 251](#)
- [Configuring Port Forwarding Without Destination Address Translation on page 254](#)
- [Example: Configuring Port Forwarding with Twice NAT on page 255](#)
- [Configuring Port Control Protocol on page 257](#)

## Configuring Static Source Translation in IPv4 Networks

To configure the translation type as **basic-nat44**, you must configure the NAT pool and rule, service set with service interface, and trace options. This topic includes the following tasks:

- [Configuring the NAT Pool and Rule on page 212](#)
- [Configuring the Service Set for NAT on page 214](#)
- [Configuring Trace Options on page 215](#)
- [Sample Configuration - Static Source NAT Using a Static Pool With An Address Prefix And An Address Range on page 216](#)
- [Sample Configuration - Static Source Nat for One-To-One Mapping Between a Private Subnet and a Public Subnet on page 217](#)

---

### Configuring the NAT Pool and Rule

To configure the NAT pool, rule, and term:

1. In configuration mode, go to the **[edit services nat]** hierarchy level.

```
[edit]
user@host# edit services nat
```

2. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool name address address
```

In the following example, the pool name is **src\_pool** and the address is **10.10.10.2/32**.

```
[edit services nat]
user@host# set pool src_pool address 10.10.10.2/32
```

3. Configure the NAT rule and the match direction.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction
```

In the following example, the NAT rule name is **rule-basic-nat44** and the match direction is **input**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 match-direction input
```

4. Configure the source address in the **from** statement.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term term-name from from
```

In the following example, the term name is **t1** and the input condition is **source-address 3.1.1.2/32**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 from source-address 3.1.1.2/32
```

5. Configure the NAT term action and properties of the translated traffic.

```
[edit services nat]
```

```
user@host# set rule rule-basic-nat44 term t1 then term-action translated-property
```

In the following example, the term action is **translated** and the property of the translated traffic is **source-pool src\_pool**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then translated source-pool src_pool
```

6. Configure the translation type.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then translated translation-type
translation-type
```

In the following example, the translation type is **basic-nat44**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then translated translation-type
basic-nat44
```

7. Verify the configuration by using the **show** command at the **[edit services nat]** hierarchy level.

```
[edit services]
user@host# show
nat {
  pool src_pool {
    address 10.10.10.2/32;
  }
  rule rule-basic-nat44 {
    match-direction input;
    term t1 {
      from {
        source-address {
          3.1.1.2/32;
        }
      }
      then {
        translated {
          source-pool src_pool;
          translation-type {
            basic-nat44;
          }
        }
      }
    }
  }
}
```



**NOTE:** If you don't configure a stateful firewall (SFW) rule for your traffic, then each packet is subjected to the following default stateful firewall rule:

- Allow any valid packets from inside to outside.
- Create forward and return flow based on packets 5-tuple.
- Allow only valid packets matching return flows from outside to inside.

The stateful firewall's packet validity checks are described in the *Stateful Firewall Anomaly Checking* in “[Junos Network Secure Overview](#)” on page 48. When a packets pass stateful firewall validity checking but are not matched by a NAT rule, they are not translated and may be forwarded if the NAT node has a valid route to the packets' destination IP addresses.

---

### Configuring the Service Set for NAT

---

To configure the service set for NAT:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```
[edit]
user@host# edit services
```

2. Configure the service set.

```
[edit services]
user@host# edit service-set service-set-name
```

In the following example, the service set name is **s1**.

```
[edit services]
user@host# edit service-set s1
```

3. For the **s1** service set, set the reference to the NAT rules configured at the **[edit services nat]** hierarchy level.

```
[edit services service-set s1]
user@host# set nat-rules rule-name
```

In the following example, the rule name is **rule-basic-nat44**.

```
[edit services service-set s1]
user@host# set nat-rules rule-basic-nat44
```

4. Configure the service interface.

```
[edit services service-set s1]
user@host# set interface-service service-interface service-interface-name
```

In the following example, the service interface name is **ms-1/2/0**.

```
[edit services service-set s1]
user@host# set interface-service service-interface ms-1/2/0
```



**NOTE:** If you have a Trio-based line card, you can configure an inline-services interface on that card:

```
[edit]
user@host# set interfaces si-0/0/0
[edit services service-set s1]
user@host# set interface-service service-interface si-0/0/0
```

5. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
    nat-rules rule-basic-nat44;
    interface-service {
        service-interface ms-1/2/0;
    }
}
```

### Configuring Trace Options

To configure the trace options:

1. In configuration mode, go to the **[edit services adaptive-services-pics]** hierarchy level.

```
[edit]
user@host# edit services adaptive-services-pics
```

2. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is **all**.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag all
```

3. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
```

```
[edit]
user@host# show services
service-set s1 {
    nat-rules rule-basic-nat44;
    interface-service {
        service-interface ms-1/2/0;
    }
}
```

```
nat {
  pool src_pool {
    address 10.10.10.2/32;
  }
  rule rule-basic-nat44 {
    match-direction input;
    term t1 {
      from {
        source-address {
          3.1.1.2/32;
        }
      }
      then {
        translated {
          source-pool src_pool;
          translation-type {
            basic-nat44;
          }
        }
      }
    }
  }
}
adaptive-services-pics {
  traceoptions {
    flag all;
  }
}
```

#### Sample Configuration - Static Source NAT Using a Static Pool With An Address Prefix And An Address Range

---

```
[edit services nat]
pool p1 {
  address 30.30.30.252/30;
  address-range low 20.20.20.1 high 20.20.20.2;
}
rule r1 {
  match-direction input;
  term {
    from {
      source-address {
        10.10.10.252/30;
      }
    }
    then {
      translated {
        source-pool p1;
        translation-type basic-nat44;
      }
    }
  }
}
```

### Sample Configuration - Static Source Nat for One-To-One Mapping Between a Private Subnet and a Public Subnet

```
[edit]
user@host# show services
service-set s1 {
    nat-rules rule-basic-nat44;
    interface-service {
        service-interface ms-1/2/0;
    }
}
nat {
    pool src_pool {
        address 10.10.10.2/32;
    }
    rule rule-basic-nat44 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    3.1.1.2/32;
                }
            }
            then {
                translated {
                    source-pool src_pool;
                    translation-type {
                        basic-nat44;
                    }
                }
            }
        }
    }
}
}
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
```

### Configuring Static Source Translation in IPv6 Networks

To configure the translation type as **basic-nat66**, you must configure the NAT pool and rule, service set with service interface, and trace options. This topic includes the following tasks:

- [Configuring the NAT Pool and Rule on page 217](#)
- [Configuring the Service Set for NAT on page 219](#)
- [Configuring Trace Options on page 220](#)

#### Configuring the NAT Pool and Rule

To configure the NAT pool, rule, and term:

1. In configuration mode, go to the **[edit services nat]** hierarchy level.

```
[edit]
user@host# edit services nat
```

2. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool name address address
```

In the following example, the pool name is **src\_pool** and the address is **10.10.10.2/32**.

```
[edit services nat]
user@host# set pool src_pool address 10.10.10.2/32
```

3. Configure the NAT rule and the match direction.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction
```

In the following example, the rule name is **rule-basic-nat66** and the match direction is **input**.

```
[edit services nat]
user@host# set rule rule-basic-nat66 match-direction input
```

4. Configure the source address in the **from** statement.

```
[edit services nat]
user@host# set rule rule-basic-nat66 term term-name from from
```

In the following, the term name is **t1** and the input condition is **source-address 10:10:10::0/96**.

```
[edit services nat]
user@host# set rule rule-basic-nat66 term t1 from source-address 10:10:10::0/96
```

5. Configure the NAT term action and properties of the translated traffic.

```
[edit services nat]
user@host# set rule rule-basic-nat66 term t1 then term-action translated-property
```

In the following example, the term action is **translated** and the property of the translated traffic is **source-pool src\_pool**.

```
[edit services nat]
user@host# set rule rule-basic-nat66 term t1 then translated source-pool src_pool
```

6. Configure the translation type.

```
[edit services nat]
user@host# set rule rule-basic-nat66 term t1 then translated translation-type
translation-type
```

In the following example, the translation type is **basic-nat66**.

```
[edit services nat]
user@host# set rule rule-basic-nat66 term t1 then translated translation-type
basic-nat66
```

7. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
```

```

nat {
  pool src_pool {
    address 10.10.10.2/32;
  }
  rule rule-basic-nat66 {
    match-direction input;
    term t1 {
      from {
        source-address {
          10:10:10::0/96;
        }
      }
      then {
        translated {
          source-pool src_pool;
          translation-type {
            basic-nat66;
          }
        }
      }
    }
  }
}

```

### Configuring the Service Set for NAT

To configure the service set for NAT:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```

[edit]
user@host# edit services

```

2. Configure the service set.

```

[edit services]
user@host# edit service-set service-set-name

```

In the following example, the service set name is **s1**.

```

[edit services]
user@host# edit service-set s1

```

3. For the **s1** service set, set the reference to the NAT rules configured at the **[edit services nat]** hierarchy level.

```

[edit services service-set s1]
user@host# set nat-rules rule-name

```

In the following example, the rule name is **rule-basic-nat66**.

```

[edit services service-set s1]
user@host# set nat-rules rule-basic-nat66

```

4. Configure the service interface.

```

[edit services service-set s1]
user@host# set interface-service service-interface service-interface-name

```

In the following example, the service interface name is **sp-1/2/0**.

```

[edit services service-set s1]

```

```
user@host# set interface-service service-interface sp-1/2/0
```

5. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
    nat-rules rule-basic-nat66;
    interface-service {
        service-interface sp-1/2/0;
    }
}
```

---

### Configuring Trace Options

To configure the trace options at the **[edit services adaptive-services-pics]** hierarchy level:

1. In configuration mode, go to the **[edit services adaptive-services-pics]** hierarchy level.

```
[edit]
user@host# edit services adaptive-services-pics
```

2. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is **all**.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag all
```

3. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
```

The following example configures the translation type as **basic-nat66**.

```
[edit]
user@host# show services
service-set s1 {
    nat-rules rule-basic-nat66;
    interface-service {
        service-interface sp-1/2/0;
    }
}
nat {
    pool src_pool {
        address 10.10.10.2/32;
    }
    rule rule-basic-nat66 {
        match-direction input;
        term t1 {
```

```

        from {
            source-address {
                10:10:10::0/96;
            }
        }
        then {
            translated {
                source-pool src_pool;
                translation-type {
                    basic-nat66;
                }
            }
        }
    }
}
}
}
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
}

```

## Configuring Static Destination Address Translation in IPv4 Networks

In IPv4 networks, destination address translation is a mechanism used to implement address translation for destination traffic without port mapping. To use destination address translation, the size of the pool address space must be greater than or equal to the destination address space. You must specify a name for the **destination-pool** statement, which can contain multiple addresses, ranges, or prefixes, as long as the number of NAT addresses in the pool is larger than the number of destination addresses in the **from** statement.

To configure destination address translation in IPv4 networks:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```

[edit]
user@host# edit services

```

2. Configure the service set and the NAT rule.

```

[edit services]
user@host# set service-set service-set-name nat-rules rule-name

```

In the following example, the name of the service set is **s1** and the name of the NAT rule is **rule-dnat44**.

```

[edit services]
user@host# set service-set s1 nat-rules rule-dnat44

```

3. Go to the **[interface-service]** hierarchy level of the service set.

```

[edit services]
user@host# edit service-set s1 interface-service

```

4. Configure the service interface.

```

[edit services service-set s1 interface-service]
user@host# set service-interface service-interface-name

```

In the following example, the name of the service interface is **ms-0/1/0**.



**NOTE:** If the service interface is not present in the router, or the specified interface is not functional, the following command can result in an error.

```
[edit services service-set s1 interface-service]
user@host# set service-interface ms-0/1/0
```

5. Go to the **[edit services nat]** hierarchy level. Issue the following command from the top of the services hierarchy, or use the **top** keyword.

```
[edit services service-set s1]
user@host# top edit services nat
```

6. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, **dest-pool** is used as the pool name and **4.1.1.2** as the address.

```
user@host# set pool dest-pool address 4.1.1.2
```

7. Configure the rule, match direction, term, and destination address.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name from
destination-address address
```

In the following example, the name of the rule is **rule-dnat44**, the match direction is **input**, the name of the term is **t1**, and the address is **20.20.20.20**.

```
[edit services nat]
user@host# set rule rule-dnat44 match-direction input term t1 from
destination-address 20.20.20.20
```

8. Go to the **[edit services nat rule rule-dnat44 term t1]** hierarchy level.

```
[edit services nat]
user@host# edit rule rule-dnat44 term t1
```

9. Configure the destination pool and the translation type.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then translated destination-pool dest-pool-name translation-type
translation-type
```

In the following example, the destination pool name is **dest-pool**, and the translation type is **dnat-44**.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then translated destination-pool dest-pool translation-type dnat-44
```

10. Go to the **[edit services adaptive-services-pics]** hierarchy level. In the following command, the **top** keyword ensures that the command is run from the top of the hierarchy.

```
[edit services nat rule rule-dnat44 term t1]
user@host# top edit services adaptive-services-pics
```

11. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is configured as **all**.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag all
```

12. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
  nat-rules rule-dnat44;
  interface-service {
    service-interface ms-0/1/0;
  }
}
nat {
  pool dest-pool {
    address 4.1.1.2/32;
  }
  rule rule-dnat44 {
    match-direction input;
    term t1 {
      from {
        destination-address {
          20.20.20.20/32;
        }
      }
      then {
        translated {
          destination-pool dest-pool;
          translation-type {
            dnat-44;
          }
        }
      }
    }
  }
}
adaptive-services-pics {
  traceoptions {
    flag all;
  }
}
```

The following example configures the translation type as **dnat-44**.

```
[edit services]
user@host# show
service-set s1 {
  nat-rules rule-dnat44;
  interface-service {
    service-interface ms-0/1/0;
  }
}
nat {
  pool dest-pool {
```

```

        address 4.1.1.2/32;
    }
    rule rule-dnat44 {
        match-direction input;
        term t1 {
            from {
                destination-address {
                    20.20.20.20/32;
                }
            }
            then {
                translated {
                    destination-pool dest-pool;
                    translation-type {
                        dnat-44;
                    }
                }
            }
        }
    }
}
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}

```

In the following configuration, **term1** configures source address translation for traffic from any private address to any public address. The translation is applied for all services. **term2** performs destination address translation for Hypertext Transfer Protocol (HTTP) traffic from any public address to the server's virtual IP address. The virtual server IP address is translated to an internal IP address.

```

[edit services nat]
rule my-nat-rule {
    match-direction input;
    term my-term1 {
        from {
            source-address private;
            destination-address public;
        }
        then {
            translated {
                source-pool my-pool; # pick address from a pool
                translation-type napt-44; # dynamic NAT with port translation
            }
        }
    }
    term my-term2 {
        from {
            destination-address 192.168.137.3; # my server's virtual address
            application http;
        }
        then {
            translated {
                destination-pool nat-pool-name;
                translation-type dnat-44; # static destination NAT
            }
        }
    }
}

```

```

    }
  }
}

```

The following configuration performs NAT using the destination prefix **20.20.10.0/32** without defining a pool.

```

[edit services nat]
rule src-nat {
  match-direction input;
  term t1 {
    from {
      destination-address 10.10.10.10/32;
    }
    then {
      translation-type dnat44;
      destination-prefix 20.20.10.0/24;
    }
  }
}
}

```

## Configuring Dynamic Address-Only Source Translation in IPv4 Networks

In IPv4 networks, dynamic address translation (dynamic NAT) is a mechanism to dynamically translate the destination traffic without port mapping. To use dynamic NAT, you must specify a source pool name, which includes an address configuration.

To configure dynamic NAT in IPv4 networks:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```

[edit]
user@host# edit services

```

2. Configure the service set and NAT rule.

```

[edit services]
user@host# set service-set service-set-name nat-rules rule-name

```

In the following example, the name of the service set is **s1**, and the name of the NAT rule is **rule-dynamic-nat44**.

```

[edit services]
user@host# set service-set s1 nat-rules rule-dynamic-nat44

```

3. Go to the **[interface-service]** hierarchy level for the service set.

```

[edit services]
user@host# edit service-set s1 interface-service

```

4. Configure the service interface.

```

[edit services service-set s1 interface-service]
user@host# set service-interface service-interface-name

```

In the following example, the name of the service interface is **ms-0/1/0**.



**NOTE:** If the service interface is not present in the router, or the specified interface is not functional, the following command can result in an error.

```
[edit services service-set s1 interface-service]
user@host# set service-interface ms-0/1/0
```

5. Go to the **[edit services nat]** hierarchy level. Issue the following command from the top of the services hierarchy, or use the **top** keyword.

```
[edit services service-set s1 interface-service]
user@host# top edit services nat
```

6. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, the name of the pool is **source-dynamic-pool**, and the address is **10.10.10.0**.

```
[edit services nat]
user@host# set pool source-dynamic-pool address 10.10.10.0
```

7. Configure the rule, match direction, term, and source address.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name from
source-address address
```

In the following example, the name of the rule is **rule-dynamic-nat44**, the match direction is **input**, the name of the term is **t1**, and the source address is **3.1.1.0**.

```
[edit services nat]
user@host# set rule rule-dynamic-nat44 match-direction input term t1 from
source-address 3.1.1.0
```

8. Go to the **[edit rule rule-dynamic-nat-44 term t1]** hierarchy level.

```
[edit services nat]
user@host# edit rule rule-dynamic-nat44 term t1
```

9. Configure the source pool and the translation type.

```
[edit services nat rule rule-dynamic-nat44 term t1]
user@host# set then translated source-pool src-pool-name translation-type
translation-type
```

In the following example, the name of the source pool is **source-dynamic-pool** and the translation type is **dynamic-nat44**.

```
[edit services nat rule rule-dynamic-nat44 term t1]
user@host# set then translated source-pool source-dynamic-pool translation-type
dynamic-nat44
```

10. Go to the **[edit services adaptive-services-pics]** hierarchy level. In the following command, the **top** keyword ensures that the command is run from the top of the hierarchy.

```
[edit services nat rule rule-dynamic-nat44 term t1]
```

```
user@host# top edit services adaptive-services-pics
```

11. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is configured as **all**.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag all
```

12. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
    nat-rules rule-dynamic-nat44;
    interface-service {
        service-interface ms-0/1/0;
    }
}
nat {
    pool source-dynamic-pool {
        address 10.1.1.0/24;
    }
    rule rule-dynamic-nat44 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    3.1.1.0/24;
                }
            }
            then {
                translated {
                    destination-pool source-dynamic-pool;
                    translation-type {
                        dynamic-nat44;
                    }
                }
            }
        }
    }
}
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
```

The following example configures the translation type as **dynamic-nat44**.

```
[edit services]
user@host# show
service-set s1 {
    nat-rules rule-dynamic-nat44;
    interface-service {
        service-interface ms-0/1/0;
    }
}
```

```

nat {
  pool source-dynamic-pool {
    address 10.1.1.0/24;
  }
  rule rule-dynamic-nat44 {
    match-direction input;
    term t1 {
      from {
        source-address {
          3.1.1.0/24;
        }
      }
      then {
        translated {
          destination-pool source-dynamic-pool;
          translation-type {
            dynamic-nat44;
          }
        }
      }
    }
  }
}
adaptive-services-pics {
  traceoptions {
    flag all;
  }
}

```

The following configuration specifies that NAT is not performed on incoming traffic from the source address **192.168.20.24/32** by providing a NAT rule term **t0** that configures **no-translation**. Dynamic NAT is performed on all other incoming traffic, as configured by term **t1** of the NAT rule.

```

[edit services nat]
pool my-pool {
  address-range low 10.10.10.1 high 10.10.10.16;
  port-automatic;
}
rule src-nat {
  match-direction input;
  term t0 {
    from {
      source-address 192.168.20.24/32;
    }
    then {
      no-translation;
    }
  }
  term t1 {
    then {
      translated {
        translation-type dynamic-nat44;
        source-pool my-pool;
      }
    }
  }
}

```

The following configuration performs NAT using the source prefix **20.20.10.0/24** without defining a pool.

```
[edit services nat]
rule src-nat {
  match-direction input;
  term t1 {
    then {
      translation-type dynamic-nat44;
      source-prefix 20.20.10.0/24;
    }
  }
}
```

The following configuration performs NAT using the destination prefix **20.20.10.0/32** without defining a pool.

```
[edit services nat]
rule src-nat {
  match-direction input;
  term t1 {
    from {
      destination-address 10.10.10.10/32;
    }
    then {
      translation-type dnat44;
      destination-prefix 20.20.10.0/24;
    }
  }
}
```

## Configuring Dynamic Source Address and Port Translation in IPv4 Networks

Network Address Port Translation (NAPT) is a method by which many network addresses and their TCP/UDP ports are translated into a single network address and its TCP/UDP ports. This translation can be configured in both IPv4 and IPv6 networks. This section describes the steps for configuring NAPT in IPv4 networks.

To configure NAPT, you must configure a rule at the **[edit services nat]** hierarchy level for dynamically translating the source IPv4 addresses.

To configure the NAPT in IPv4 networks:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```
[edit]
user@host# edit services
```

2. Configure the service set and NAT rule.

```
[edit services]
user@host# set service-set service-set-name nat-rules rule-name
```

In the following example, the name of the service set is **s1** and the name of the NAT rule is **rule-napt-44**.

```
[edit services]
```

```
user@host# set service-set s1 nat-rules rule-napt-44
```

3. Go to the **[interface-service]** hierarchy level of the service set.

```
[edit services]
user@host# edit service-set s1 interface-service
```

4. Configure the service interface.

```
[edit services service-set s1 interface service]
user@host# set service-interface service-interface-name
```

In the following example, the name of the service interface is **ms-0/1/0**.



**NOTE:** If the service interface is not present in the router, or the specified interface is not functional, the following command can result in an error.

```
[edit services service-set s1 interface service]
user@host# set service-interface ms-0/1/0
```

5. Go to the **[edit services nat]** hierarchy level. Issue the command from the top of the services hierarchy, or use the **top** keyword.

```
[edit services service-set s1 interface service]
user@host# top edit services nat
```

6. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, the name of the pool is **napt-pool** and the address is **10.10.10.0**.

```
[edit services nat]
user@host# set pool napt-pool address 10.10.10.0
```

7. Configure the port.

```
[edit services nat]
user@host# set pool pool-name port port-type
```

In the following example, the port type is selected as **automatic**.

```
[edit services nat]
user@host# set pool napt-pool port automatic
```

8. Configure the rule and the match direction.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction
```

In the following example, the name of the rule is **rule-napt-44** and the match direction is **input**.

```
[edit services nat]
user@host# set rule rule-napt-44 match-direction input
```

9. Configure the term, the action for the translated traffic, and the translation type.

```
[edit services nat]
```

```
user@host# set rule rule-name term term-name then translated translated-action
translation-type translation-type
```

In the following example, the name of the term is **t1**, the action for the translated traffic is **translated**, the name of the source pool is **napt-pool**, and the translation type is **napt-44**.

```
[edit services nat]
user@host# set rule rule-napt-44 match-direction input term t1 then translated
source-pool napt-pool translation-type napt-44
```

10. Go to the **[edit services adaptive-services-pics]** hierarchy level. In the command, the **top** keyword ensures that the command is run from the top of the hierarchy.

```
[edit services nat]
user@host# top edit services adaptive-services-pics
```

11. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is configured as **all**.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag all
```

12. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
  nat-rules rule-napt-44;
  interface-service {
    service-interface ms-0/1/0;
  }
}
nat {
  pool napt-pool {
    address 10.10.10.0/32;
    port {
      automatic;
    }
  }
  rule rule-napt-44 {
    match-direction input;
    term t1 {
      then {
        translated {
          source-pool napt-pool;
          translation-type {
            napt-44;
          }
        }
      }
    }
  }
}
adaptive-services-pics {
  traceoptions {
    flag all;
  }
}
```

```
    }
  }
```

The following example configures the translation type as **napt-44**.

```
[edit services]
user@host# show
service-set s1 {
  nat-rules rule-napt-44;
  interface-service {
    service-interface ms-0/1/0;
  }
}
nat {
  pool napt-pool {
    address 10.10.10.0/32;
    port {
      automatic;
    }
  }
  rule rule-napt-44 {
    match-direction input;
    term t1 {
      then {
        translated {
          source-pool napt-pool;
          translation-type {
            napt-44;
          }
        }
      }
    }
  }
}
adaptive-services-pics {
  traceoptions {
    flag all;
  }
}
```

#### Dynamic Address Translation to a Small Pool with Fallback to NAT

The following configuration shows dynamic address translation from a large prefix to a small pool, translating a /24 subnet to a pool of 10 addresses. When the addresses in the source pool (**src-pool**) are exhausted, NAT is provided by the NAPT overload pool (**pat-pool**).

```
[edit services nat]
pool src-pool {
  address-range low 192.16.2.1 high 192.16.2.10;
}
pool pat-pool {
  address-range low 192.16.2.11 high 192.16.2.12;
  port automatic;
  rule myrule {
    match-direction input;
    term myterm {
      from {
        source-address 10.150.1.0/24;
      }
    }
  }
}
```

```

    then {
        translated {
            source-pool src-pool;
            overload-pool pat-pool;
            translation-type napt-44;
        }
    }
}

```

### Dynamic Address Translation with Small Pool

The following configuration shows dynamic address translation from a large prefix to a small pool, translating a /24 subnet to a pool of 10 addresses. Sessions from the first 10 host sessions are assigned an address from the pool on a first-come, first-served basis, and any additional requests are rejected. Each host with an assigned NAT can participate in multiple sessions.

```

[edit services nat]
pool my-pool {
    address-range low 10.10.10.1 high 10.10.10.10;
}
rule src-nat {
    match-direction input;
    term t1 {
        from {
            source-address 192.168.1.0/24;
        }
        then {
            translated {
                translation-type dynamic-nat44;
                source-pool my-pool;
            }
        }
    }
}

```

## Configuring Dynamic Source Address and Port Translation for IPv6 Networks

Network Address Port Translation (NAPT) is a method by which many network addresses and their TCP/UDP ports are translated into a single network address and its TCP/UDP ports. This translation can be configured in both IPv4 and IPv6 networks. This section describes the steps for configuring NAPT in IPv6 networks. For information about configuring NAPT in IPv4 networks, see [“Configuring Dynamic Source Address and Port Translation in IPv4 Networks” on page 229](#).

To configure NAPT, you must configure a rule at the **[edit services nat]** hierarchy level for dynamically translating the source IPv6 addresses.

To configure NAPT in IPv6 networks:

1. In configuration mode, go to the **[edit services nat]** hierarchy level.

```

[edit]
user@host# edit services nat

```

2. Define the pool of IPv6 source addresses that must be used for dynamic translation. For NAT, also specify port numbers when configuring the source pool.

```
[edit services nat]
user@host# set pool pool name address IPv6 source addresses
user@host# set pool pool name port source ports
```

For example:

```
[edit services nat]
user@host# set pool IPV6-NAPT-Pool address 2002::1/96
user@host# set pool IPV6-NAPT-Pool port automatic
```

3. Define a NAT rule for translating the source addresses. To do this, set the **match-direction** statement of the rule as **input**. In addition, define a term that uses **napt-66** as the translation type for translating the addresses of the pool defined in the previous step.

```
[edit services nat]
user@host# set rule rule name match-direction input
user@host# set rule rule name term term name then translated source-pool pool name
user@host# set rule rule name term term name then translated translation-type napt-66
```

For example:

```
[edit services nat]
user@host# set rule IPV6-NAPT-Rule match-direction input
user@host# set rule IPV6-NAPT-Rule term t1 then translated source-pool
    IPV6-NAPT-Pool
user@host# set rule IPV6-NAPT-Rule term t1 then translated translation-type napt-66
```

4. Enter the **up** command to navigate to the **[edit services]** hierarchy level.

```
[edit services nat]
user@host# up
```

5. Define a service set to specify the services interface that must be used, and reference the NAT rule implemented for NATP translation.

```
[edit services]
user@host# set service-set service-set name interface- service service-interface
    services interface
user@host# set service-set service-set name nat-rules rule name
```

For example:

```
[edit services]
user@host# set service-set IPV6-NAPT-ServiceSet interface-service service-interface
    ms-0/1/0
user@host# set service-set IPV6-NAPT-ServiceSet nat-rules IPV6-NAPT-Rule
```

6. Define the trace options for the adaptive services PIC.

```
[edit services]
user@host# set adaptive-services-pics traceoptions flag tracing parameter
```

For example:

```
[edit services]
user@host# set adaptive-services-pics traceoptions flag all
```

The following example configures dynamic source (address and port) translation or NAT for an IPv6 network.

```
[edit services]
user@host# show
    service-set IPV6-NAPT-ServiceSet {
        nat-rules IPV6-NAPT-Rule;
        interface-service {
            service-interface ms-0/1/0;
        }
    }
    nat {
        pool IPV6-NAPT-Pool {
            address 2002::1/96;
            port automatic;
        }
        rule IPV6-NAPT-Rule {
            match-direction input;
            term term1 {
                then {
                    translated {
                        source-pool IPV6-NAPT-Pool;
                        translation-type {
                            napt-66;
                        }
                    }
                }
            }
        }
    }
    adaptive-services-pics {
        traceoptions {
            flag all;
        }
    }
}
```

## Configuring Secured Port Block Allocation

To configure secured port block allocation:

1. At the `[edit services nat pool poolname]` hierarchy level, create a pool.

```
user@host# edit services nat pool poolname
```

For example:

```
user@host# edit services nat pool pba-pool1
```

2. Define the range of addresses to be translated, specifying the upper and lower limits of the range or an address prefix that describes the range.

```
[edit services nat pool pba-pool1]
user@host# set address-range low address high address
```

Or

```
user@host# set address address-prefix
```

For example:

```
[edit services nat pool pba-pool1]
```

```
user@host# set address 203.0.113.0/24
```

3. Define the range of ports to be used in the translation, or use automatic port assignment by the Junos OS. You can optionally specify random assignment of ports (sequential assignment is the default).

```
[edit services nat pool pba-pool1]  
user@host# set port range low address high address random
```

Or

```
user@host# set port automatic random-allocation
```

For example:

```
[edit services nat pool pba-pool1]  
user@host# set port range low 256 high 511 random
```

Or

```
[edit services nat pool pba-pool1]  
user@host# set port automatic random-allocation
```



**NOTE:** When you configure a port range, the range should be a multiple of the port block-size value (see Step 4). When the NAT pool port range is *not* a multiple of the port block-size value, the number of ports or port-blocks that are effectively available for use is less than the configured number of ports and port-blocks. The port block allocation mechanism uses ports in the range 0 through 1023 of a NAT address.

When you configure automatic assignment of ports, the available port range for allocation is 1024 through 65535. Automatic allocation can result in no ports being available for use. Use the `show services nat pool` command on the Routing Engine after you configure the port block allocation method to determine the number of ports and port blocks available for allocation to users.

4. Configure secured port block allocation. Specify **active-block-timeout**, **block-size**, and **max-blocks-per-address**, or accept the default values for those options.

```
[edit services nat pool pba-pool1]  
user@host# set secured-port-block-allocation active-block-timeout  
active-block-timeout block-size block-size max-blocks-per-address  
max-blocks-per-address
```

For example:

```
[edit services nat pool pba-pool1]  
user@host# set secured-port-block-allocation active-block-timeout 120 block-size  
256 max-blocks-per-address 12
```



**NOTE:** In order for secured-port-block-allocation configuration changes to take effect, you must reboot the services PIC whenever you change any of the following nat pool options:

- *pool-name*
- address or address-range
- port range
- port secured-port-block-allocation block-size
- port secured-port-block-allocation max-blocks-per-address.
- port secured-port-block-allocation active-block-timeout.
- from hierarchy in the nat rule

Related  
Documentation

- [Network Address Translation Configuration Overview on page 191](#)

## Configuring Deterministic Port Block Allocation

To configure deterministic port block allocation:

1. At to the `[edit services nat pool poolname]` hierarchy level, create a pool.

```
user@host# edit services nat pool poolname
```

For example:

```
user@host# edit services nat pool pba-pool2
```

2. Define the range of addresses to be translated, specifying the upper and lower limits of the range or an address prefix that describes the range.

```
[edit services nat pool pba-pool1]
user@host# set address-range low address high address
```

Or

```
user@host# set address address-prefix
```

For example:

```
[edit services nat pool pba-pool1]
user@host# set address-range low 32.32.32.1 high 32.32.32.253
```

3. Specify automatic port assignment by the Junos OS.

```
[edit services nat pool pba-pool1]
user@host# set port automatic
```

4. Configure deterministic port block allocation. Specify **block-size** or accept the default value of 512.

. You can also specify **include-boundary-addresses** if you want the lowest and highest addresses in the source address range of a NAT rule to be translated when the NAT pool is used.

```
[edit services nat pool pba-pool1]
user@host# set port deterministic-port-block-allocation block-size block-size
include-boundary-addresses
```

For example:

```
[edit services nat pool pba-pool1]
user@host# set port deterministic-port-block-allocation block-size 256
```



**NOTE:** In order for deterministic-port-block-allocation configuration changes to take effect, you must reboot the services PIC whenever you change any of the following nat pool options:

- address or address-range
- port range
- port deterministic-port-block-allocation block-size

**Related Documentation**

- [Network Address Translation Configuration Overview on page 191](#)

## Configuring Stateful NAT64

Stateful NAT64 is a mechanism used to move to an IPv6 network and at the same time deal with IPv4 address depletion. By allowing IPv6-only clients to contact IPv4 servers using unicast UDP, TCP, or ICMP, several IPv6-only clients can share the same public IPv4 server address. To allow sharing of the IPv4 server address, stateful NAT64 translates incoming IPv6 packets into IPv4, and vice versa.

To configure stateful NAT64, you must configure a rule at the **[edit services nat]** hierarchy level for translating the source address dynamically and the destination address statically.



**BEST PRACTICE:** When you configure the service set that includes your NAT rule, include the set `stateful-nat64 clear-dont-fragment-bit` at the **[edit services service-set service-set-name]** hierarchy level. This clears the DF (don't fragment) bit in order to prevent unnecessary creation of an IPv6 fragmentation header when translating IPv4 packets that are less than 1280 bytes. RFC 6145, *IP/ICMP Translation Algorithm*, provides a full discussion of the use of the DF flag to control generation of fragmentation headers. For more information on service sets for NAT, see [“Configuring Service Sets for Network Address Translation” on page 209](#).

To configure stateful NAT64:

1. In configuration mode, go to the **[edit services nat]** hierarchy level.

```
[edit]
user@host# edit services nat
```

2. Define the pool of source addresses to be used for dynamic translation.

```
[edit services nat]
user@host# set pool pool name address source addresses
user@host# set pool pool name port source ports
```

For example:

```
[edit services nat]
user@host# set pool src-pool-nat64 address 203.0.113.0/24
user@host# set pool src-pool-nat64 port automatic
```

3. Define a NAT rule for translating the source addresses. Set the **match-direction** statement of the rule as **input**. Then define a term that uses **stateful-nat64** as the translation type for translating the addresses of the pool defined in the previous step.

```
[edit services nat]
user@host# set rule rule name match-direction input
user@host# set rule rule name term term name from source-address source address
user@host# set rule rule name term term name from destination-address destination address
user@host# set rule rule name term term name then translated source-pool pool name
user@host# set rule rule name term term name then translated destination-prefix destination prefix
user@host# set rule rule name term term name then translated translation-type stateful-nat64
```

For example:

```
[edit services nat]
user@host# set rule stateful-nat64 match-direction input
user@host# set rule stateful-nat64 term t1 from source-address 2001:DB8::0/96
user@host# set rule stateful-nat64 term t1 from destination-address 64:FF9B::/96
user@host# set rule stateful-nat64 term t1 then translated source-pool src-pool-nat64
user@host# set rule stateful-nat64 term t1 then translated destination-prefix 64:FF9B::/96
user@host# set rule stateful-nat64 term t1 then translated translation-type stateful-nat64
```

The following example configures dynamic source address (IPv6-to-IPv4) and static destination address (IPv6-to-IPv4) translation.

```
[edit services]
user@host# show
nat {
  pool src-pool-nat64 {
    address 203.0.113.0/24;
    port {
      automatic;
    }
  }
  rule stateful-nat64 {
    match-direction input;
    term t1 {
      from {
        source-address {
          2001:db8::0/96;
        }
        destination-address {
          64:ff9b::/96;
        }
      }
    }
  }
}
```

```
        then {
            translated {
                source-pool src-pool-nat64;
                destination-prefix 64:ff9b::/96;
                translation-type {
                    stateful-nat64;
                }
            }
        }
    }
}
service-set sset-nat64 {
    nat-options {
        stateful-nat64 {
            clear-dont-fragment-bit;
        }
    }
    service-set-options;
    nat-rules stateful-nat64;
    interface-service {
        service-interface ms-0/1/0;
    }
}
```

## Configuring Protocol Translation Between IPv6 and IPv4 Networks - NAT-PT

To configure the translation type as **basic-nat-pt**, you must configure the DNS ALG application, the NAT pools and rules, a service set with a service interface, and trace options. This topic includes the following tasks:

- [Configuring the DNS ALG Application on page 240](#)
- [Configuring the NAT Pool and NAT Rule on page 241](#)
- [Configuring the Service Set for NAT on page 244](#)
- [Configuring Trace Options on page 245](#)

### Configuring the DNS ALG Application

---

To configure the DNS ALG application:

1. In configuration mode, go to the **[edit applications]** hierarchy level.

```
[edit]
user@host# edit applications
```

2. Configure the ALG to which the DNS traffic is destined at the **[edit applications]** hierarchy level. Define the application name and specify the application protocol to use in match conditions in the first NAT rule or term.

```
[edit applications]
user@host# set application application-name application-protocol application-protocol
```

In the following example, the application name is **dns-alg** and application protocol is **dns**.

```
[edit applications]
user@host# set application dns-alg application-protocol dns
```

3. Verify the configuration by using the **show** command at the **[edit applications]** hierarchy level.

```
[edit applications]
user@host# show
application dns-alg {
    application-protocol dns;
}
```

### Configuring the NAT Pool and NAT Rule

To configure the NAT pool and NAT rule:

1. In configuration mode, go to the **[edit services nat]** hierarchy level.

```
[edit]
user@host# edit services nat
```

2. Configure the NAT pool and its address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, the name of the NAT pool is **p1** and the address is **10.10.10.2/32**.

```
[edit services nat]
user@host# set pool p1 address 10.10.10.2/32
```

3. Configure the source pool and its address.

```
[edit services nat]
user@host# set pool source-pool-name address address
```

In the following example, the name of the source pool is **src\_pool0** and the source pool address is **20.1.1.1/32**.

```
[edit services nat]
user@host# set pool src_pool0 address 20.1.1.1/32
```

4. Configure the destination pool and its address.

```
[edit services nat]
user@host# set pool destination-pool-name address address
```

In the following example, the name of the destination pool is **dst\_pool0** and the destination pool address is **50.1.1.2/32**.

```
[edit services nat]
user@host# set pool dst_pool0 address 50.1.1.2/32
```

5. Configure the rule and the match direction.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction
```

In the following example, the rule name is **rule-basic-nat-pt** and the match direction is **input**.

```
[edit services nat]
user@host# set rule basic-nat-pt match-direction input
```

6. Configure the term and the input conditions for the NAT term.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term term from from
```

In the following example, the term is **t1** and the input conditions are **source-address 2000::2/128**, **destination-address 4000::2/128**, and **applications dns\_alg**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 from source-address 2000::2/128
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 from destination-address 4000::2/128
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 from applications dns_alg
```

7. Configure the NAT term action and the properties of the translated traffic.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 then term-action translated-property
```

In the following example, the term action is **translated** and the properties of the translated traffic are **source-pool src\_pool0**, **destination-pool dst\_pool0**, and **dns-alg-prefix 10:10:10::0/96**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 then translated source-pool src_pool0
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 then translated destination-pool
dst_pool0
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 then translated dns-alg-prefix
10:10:10::0/96
```

8. Configure the translation type.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 then translated translation-type
translation-type
```

In the following example, the translation type is **basic-nat-pt**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 then translated translation-type
basic-nat-pt
```

9. Configure another term and the input conditions for the NAT term.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term term-name from from
```

In the following example, the term name is **t2** and the input conditions are **source-address 2000::2/128** and **destination-address 10:10:10::0/96**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 from source-address 2000::2/128
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 from destination-address 10:10:10::0/96
```

10. Configure the NAT term action and the property of the translated traffic.

```
[edit services nat]
```

```
user@host# set rule rule-basic-nat-pt term t2 then term-action translated-property
```

In the following example, the term action is **translated** and the property of the translated traffic is **source-prefix 19.19.19.1/32**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 then translated source-prefix
19.19.19.1/32
```

11. Configure the translation type.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 then translated translation-type
translation-type
```

In the following example, the translation type is **basic-nat-pt**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 then translated translation-type
basic-nat-pt
```

12. Verify the configuration by using the **show** command at the **[edit services nat]** hierarchy level.

```
[edit services nat]
user@host# show
pool p1 {
    address 10.10.10.2/32;
}
pool src_pool0 {
    address 20.1.1.1/32;
}
pool dst_pool0 {
    address 50.1.1.2/32;
}
rule rule-basic-nat-pt {
    match-direction input;
    term t1 {
        from {
            source-address {
                2000::2/128;
            }
            destination-address {
                4000::2/128;
            }
            applications dns_alg;
        }
        then {
            translated {
                source-pool src_pool0;
                destination-pool dst_pool0;
                dns-alg-prefix 10:10:10::0/96;
                translation-type {
                    basic-nat-pt;
                }
            }
        }
    }
    term t2 {
        from {
            source-address {
                2000::2/128;
            }

```

```
    }
    destination-address {
        10:10:10::0/96;
    }
}
then {
    translated {
        source-prefix 19.19.19.1/32;
        translation-type {
            basic-nat-pt;
        }
    }
}
}
```

---

### Configuring the Service Set for NAT

To configure the service set for NAT:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```
[edit]
user@host# edit services
```

2. Configure the service set.

```
[edit services]
user@host# edit service-set service-set-name
```

In the following example, the name of the service set is **ss\_dns**.

```
[edit services]
user@host# edit service-set ss_dns
```

3. Configure the service set with NAT rules.

```
[edit services service-set ss_dns]
user@host# set nat-rules rule-name
```

In the following example, the rule name is **rule-basic-nat-pt**.

```
[edit services service-set ss_dns]
user@host# set nat-rules rule-basic-nat-pt
```

4. Configure the service interface.

```
[edit services service-set ss_dns]
user@host# set interface-service service-interface service-interface-name
```

In the following example, the name of service interface is **sp-1/2/0**.

```
[edit services service-set ss_dns]
user@host# set interface-service service-interface sp-1/2/0
```

5. Verify the configuration by using the **show services** command from the **[edit]** hierarchy level.

```
[edit]
user@host# show services
  service-set ss_dns {
    nat-rules rule-basic-nat-pt;
```

```

        interface-service {
            service-interface sp-1/2/0;
        }
    }

```

### Configuring Trace Options

To configure the trace options:

1. In configuration mode, go to the **[edit services adaptive-services-pics]** hierarchy level.

```

[edit]
user@host# edit services adaptive-services-pics

```

2. Configure the trace options.

```

[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter

```

In the following example, the tracing parameter is **all**.

```

[edit services adaptive-services-pics]
user@host# set traceoptions flag all

```

3. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```

[edit services]
user@host# show
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}

```

The following example configures the translation type as **basic-nat-pt**.

```

[edit]
user@host# show services
service-set ss_dns {
    nat-rules rule-basic-nat-pt;
    interface-service {
        service-interface sp-1/2/0;
    }
}
nat {
    pool p1 {
        address 10.10.10.2/32;
    }
    pool src_pool0 {
        address 20.1.1.1/32;
    }
    pool dst_pool0 {
        address 50.1.1.2/32;
    }
    rule rule-basic-nat-pt {
        match-direction input;
        term t1 {
            from {
                source-address {

```

```

        2000::2/128;
    }
    destination-address {
        4000::2/128;
    }
    applications dns_alg;
}
then {
    translated {
        source-pool src_pool0;
        destination-pool dst_pool0;
        dns-arg-prefix 10:10:10::0/96;
        translation-type {
            basic-nat-pt;
        }
    }
}
}
term t2 {
    from {
        source-address {
            2000::2/128;
        }
        destination-address {
            10:10:10::0/96;
        }
    }
    then {
        translated {
            source-prefix 19.19.19.1/32;
            translation-type {
                basic-nat-pt;
            }
        }
    }
}
}
}
}
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
}

```

### Example: Assigning Addresses from a Dynamic Pool for Static Use

The following configuration statically assigns a subset of addresses that are configured as part of a dynamic pool (**dynamic-pool**) to two separate static pools (**static-pool** and **static-pool2**).

```

[edit services nat]
pool dynamic-pool {
    address 20.20.10.0/24;
}
pool static-pool {
    address-range low 20.20.10.10 high 10.20.10.12;
}
pool static-pool2 {
    address 20.20.10.15/32;
}

```

```

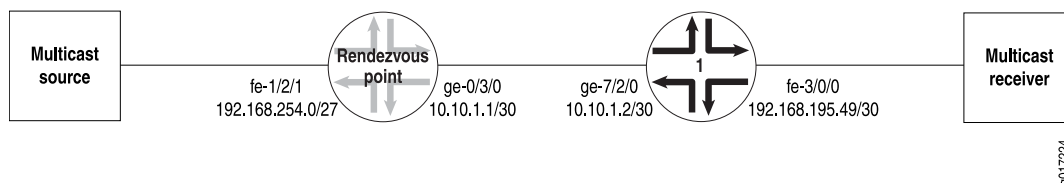
}
rule src-nat {
  match-direction input;
  term t1 {
    from {
      source-address 30.30.30.0/24;
    }
    then {
      translation-type dynamic-nat44;
      source-pool dynamic-pool;
    }
  }
  term t2 {
    from {
      source-address 10.10.10.2;
    }
    then {
      translation-type basic-nat44;
      source-pool static-pool;
    }
  }
  term t3 {
    from {
      source-address 10.10.10.10;
    }
    then {
      translation-type basic-nat44;
      source-pool static-pool2;
    }
  }
}

```

### Example: Configuring NAT for Multicast Traffic

Figure 12 on page 247 illustrates the network setup for the following configuration, which allows IP multicast traffic to be sent to the Multiservices PIC.

Figure 12: Configuring NAT for Multicast Traffic



- [Rendezvous Point Configuration on page 247](#)
- [Router 1 Configuration on page 250](#)

#### Rendezvous Point Configuration

On the rendezvous point (RP), all incoming traffic from the multicast source at **192.168.254.0/27** is sent to the static NAT pool **mcast\_pool**, where its source is translated to **20.20.20.0/27**. The service set **nat\_ss** is a next-hop service set that allows IP multicast traffic to be sent to the Multiservices DPC or Multiservices PIC. The inside interface on the PIC is **ms-1/1/0.1** and the outside interface is **ms-1/1/0.2**.

```
[edit services]
nat {
  pool mcast_pool {
    address 20.20.20.0/27;
  }
  rule nat_rule_1 {
    match-direction input;
    term 1 {
      from {
        source-address 192.168.254.0/27;
      }
    }
    then {
      translated {
        source-pool mcast_pool;
        translation-type basic-nat44;
      }
      syslog;
    }
  }
}
service-set nat_ss {
  allow-multicast;
  nat-rules nat_rule_1;
  next-hop-service {
    inside-service-interface ms-1/1/0.1;
    outside-service-interface ms-1/1/0.2;
  }
}
```

The Gigabit Ethernet interface **ge-0/3/0** carries traffic out of the RP to Router 1. The multiservices interface **ms-1/1/0** has two logical interfaces: **unit 1** is the inside interface for next-hop services and **unit 2** is the outside interface for next-hop services. Multicast source traffic comes in on the Fast Ethernet interface **fe-1/2/1**, which has the firewall filter **fbf** applied to incoming traffic.

```
[edit interfaces]
ge-0/3/0 {
  unit 0 {
    family inet {
      address 10.10.1.1/30;
    }
  }
}
ms-1/1/0 {
  unit 0 {
    family inet;
  }
  unit 1 {
    family inet;
    service-domain inside;
  }
  unit 2 {
    family inet;
    service-domain outside;
  }
}
```

```

    }
  }
  fe-1/2/1 {
    unit 0 {
      family inet {
        filter {
          input fbf;
        }
        address 192.168.254.27/27;
      }
    }
  }
}

```

Multicast packets can only be directed to the Multiservices DPC or the Multiservices PIC using a next-hop service set. In the case of NAT, you must also configure a VPN routing and forwarding instance (VRF). Therefore, the routing instance **stage** is created as a “dummy” forwarding instance. To direct incoming packets to **stage**, you configure filter-based forwarding through a firewall filter called **fbf**, which is applied to the incoming interface **fe-1/2/1**. A lookup is performed in **stage.inet.0**, which has a multicast static route that is installed with the next hop pointing to the PIC's inside interface. All multicast traffic matching this route is sent to the PIC.

```

[edit firewall]
filter fbf {
  term 1 {
    then {
      routing-instance stage;
    }
  }
}

```

The routing instance **stage** forwards IP multicast traffic to the inside interface **ms-1/1/0.1** on the Multiservices DPC or Multiservices PIC:

```

[edit]
routing-instances stage {
  instance-type forwarding;
  routing-options {
    static {
      route 224.0.0.0/4 next-hop ms-1/1/0.1;
    }
  }
}

```

You enable OSPF and Protocol Independent Multicast (PIM) on the Fast Ethernet and Gigabit Ethernet logical interfaces over which IP multicast traffic enters and leaves the RP. You also enable PIM on the outside interface (**ms-1/1/0.2**) of the next-hop service set.

```

[edit protocols]
ospf {
  area 0.0.0.0 {
    interface fe-1/2/1.0 {
      passive;
    }
    interface lo0.0;
  }
}

```

```
        interface ge-0/3/0.0;
    }
}
pim {
    rp {
        local {
            address 10.255.14.160;
        }
    }
}
interface fe-1/2/1.0;
interface lo0.0;
interface ge-0/3/0.0;
interface ms-1/1/0.2;
}
```

As with any filter-based forwarding configuration, in order for the static route in the forwarding instance **stage** to have a reachable next hop, you must configure routing table groups so that all interface routes are copied from **inet.0** to the routing table in the forwarding instance. You configure routing tables **inet.0** and **stage.inet.0** as members of **fbf\_rib\_group**, so that all interface routes are imported into both tables.

```
[edit routing-options]
interface-routes {
    rib-group inet fbf_rib_group;
}
rib-groups fbf_rib_group {
    import-rib [ inet.0 stage.inet.0 ];
}
multicast {
    rpf-check-policy no_rpf;
}
```

Reverse path forwarding (RPF) checking must be disabled for the multicast group on which source NAT is applied. You can disable RPF checking for specific multicast groups by configuring a policy similar to the one in the example that follows. In this case, the **no\_rpf** policy disables RPF check for multicast groups belonging to **224.0.0.0/4**.

```
[edit policy-options]
policy-statement no_rpf {
    term 1 {
        from {
            route-filter 224.0.0.0/4 orlonger;
        }
        then reject;
    }
}
```

---

### Router 1 Configuration

The Internet Group Management Protocol (IGMP), OSPF, and PIM configuration on Router 1 is as follows. Because of IGMP static group configuration, traffic is forwarded out **fe-3/0/0.0** to the multicast receiver without receiving membership reports from host members.

```
[edit protocols]
igmp {
```

```

interface fe-3/0/0.0 {
}
}
ospf {
  area 0.0.0.0 {
    interface fe-3/0/0.0 {
      passive;
    }
    interface lo0.0;
    interface ge-7/2/0.0;
  }
  pim {
    rp {
      static {
        address 10.255.14.160;
      }
    }
    interface fe-3/0/0.0;
    interface lo0.0;
    interface ge-7/2/0.0;
  }
}

```

The routing option creates a static route to the NAT pool, **mcast\_pool**, on the RP.

```

[edit routing-options]
static {
  route 20.20.20.0/27 next-hop 10.10.1.1;
}

```

## Configuring Port Forwarding for Static Destination Address Translation

Starting with Junos OS Release 11.4, you can map an external IP address and port with an IP address and port in a private network. This allows the destination address and port of a packet to be changed to reach the correct host in a Network Address Translation (NAT) gateway. The translation facilitates reaching a host within a masqueraded, typically private, network, based on the port number on which the packet was received from the originating host. Port forwarding allows remote computers, such as public machines on the Internet, to connect to a non-standard port (port other than 80) of a specific computer within a private network. An example of this type of destination is the host of a public HTTP server within a private network. Port forwarding is supported only with **dnat-44** and **twice-napt-44** on IPv4 networks. Port forwarding works only with the FTP application-level gateway (ALG). Port forwarding also supports endpoint-independent mapping (EIM), endpoint-independent filtering (EIF), and address pooling paired (APP). Port forwarding has no support for technologies such as IPv6 rapid deployment (6rd) and dual-stack lite (DS-Lite) that offer IPv6 services over IPv4 infrastructure.

To configure destination address translation with port forwarding in IPv4 networks:

1. In configuration mode, go to the **[edit services nat]** hierarchy level.

```

[edit]
user@host# edit services nat

```

2. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, **dest-pool** is used as the pool name and **4.1.1.2** as the address.

```
user@host# set pool dest-pool address 4.1.1.2
```

3. Configure the rule, match direction, term, and destination address.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name from
destination-address address
```

In the following example, the name of the rule is **rule-dnat44**, the match direction is **input**, the name of the term is **t1**, and the address is **20.20.20.20**.

```
[edit services nat]
user@host# set rule rule-dnat44 match-direction input term t1 from
destination-address 20.20.20.20
```

4. Configure the destination port range.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name from
destination-port range high | low
```

In the following example, the upper port range is **50** and the lower port range is **20**.

```
[edit services nat]
user@host# set rule rule-dnat44 match-direction input term t1 from destination-port
range high 50 low 20
```

5. Go to the **[edit services nat rule rule-dnat44 term t1]** hierarchy level.

```
[edit services nat]
user@host# edit rule rule-dnat44 term t1
```

6. Configure the destination pool.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then translated destination-pool dest-pool-name
```

In the following example, the destination pool name is **dest-pool**, and the translation type is **dnat-44**.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then translated destination-pool dest-pool
```

7. Configure the mapping for port forwarding and the translation type.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then port-forwarding-mappings map-name translation-type
translation-type
```

In the following example, the port forwarding map name is **map1**, and the translation type is **dnat-44**.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then port-forwarding-mappings map1 translation-type dnat-44
```

8. Go to the **[edit services nat port-forwarding map1]** hierarchy level.

```
[edit services nat]
user@host# edit port-forwarding map1
```

## 9. Configure the mapping for port forwarding.

```
[edit port-forwarding map1]
user@host# set destined-port port-id
user@host# set translated-port port-id
```

In the following example, the destination port is 45 and the translated port is 23.

```
[edit port-forwarding map1]
user@host# set destined-port 23
user@host# set translated-port 45
```

**NOTE:**

- Multiple port mappings are supported with port forwarding. Up to 32 port maps can be configured for port forwarding.
- The destination port should not overlap the port range configured for NAT.

10. Verify the configuration by using the **show** command at the **[edit services nat]** hierarchy level.

```
[edit services]
user@host# show
nat {
  pool dest-pool {
    address 4.1.1.2/32;
  }
  rule rule-dnat44 {
    match-direction input;
    term t1 {
      from {
        destination-address {
          20.20.20.20/32;
        }
        destination-port {
          range low 20 high 50;
        }
      }
      then {
        port-forwarding-mappings map1;
        translated {
          destination-pool dest-pool;
          translation-type {
            dnat-44;
          }
        }
      }
    }
  }
}
port-forwarding map1 {
  destined-port 45;
  translated-port 23;
}
```



---

**NOTE:**

- A similar configuration is possible with twice NAT for IPv4. See [“Example: Configuring Port Forwarding with Twice NAT” on page 255](#).
  - Port forwarding and stateful firewall can be configured together. Stateful firewall has precedence over port forwarding.
- 

**Related Documentation**

- [Configuring Static Destination Address Translation in IPv4 Networks on page 221](#)

## Configuring Port Forwarding Without Destination Address Translation

Starting with Junos OS Release 12.1, you can configure port forwarding without translating a destination address.

To configure port forwarding without destination address translation in IPv4 networks:

1. In configuration mode, go to the **[edit services nat]** hierarchy level.

```
[edit]
user@host# edit services nat
```

2. Configure the rule, match direction, term, and destination address.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name
```

In the following example, the name of the rule is **rule-port-forwarding**, the match direction is **input**, and the name of the term is **t1**.

```
[edit services nat]
user@host# set rule rule-port-forwarding match-direction input term t1
```

3. Go to the **[edit services nat rule rule-port-forwarding term t1]** hierarchy level.

```
[edit services nat]
user@host# edit rule rule-port-forwarding term t1
```

4. Specify that there is no address translation for this rule.

```
[edit services nat rule rule-port-forwarding term t1]
user@host# set then no-translation
```

5. Configure the mapping for port forwarding and the translation type.

```
[edit services nat rule rule-port-forwarding term t1]
user@host# set then port-forwarding-mappings map-name
```

In the following example, the port forwarding map name is **map1**.

```
[edit services nat rule rule-port-forwarding term t1]
user@host# set then port-forwarding-mappings map1
```

6. Go to the **[edit services nat port-forwarding map1]** hierarchy level.

```
[edit services nat]
user@host# edit port-forwarding map1
```

7. Configure the mapping for port forwarding.

```
[edit port-forwarding map1]
user@host# set destined-port port-id
user@host# set translated-port port-id
```

In the following example, the destination port is 45 and the translated port is 23.

```
[edit port-forwarding map1]
user@host# set destined-port 23
user@host# set translated-port 45
```



**NOTE:**

- Multiple port mappings are supported with port forwarding. Up to 32 port maps can be configured for port forwarding.
- The destination port should not overlap the port range configured for NAT.

8. Verify the configuration by using the **show** command at the **[edit services nat]** hierarchy level.

```
[edit services]
user@host# show
nat {
  rule rule-port-forwarding {
    match-direction input;
    term t1 {
      then {
        port-forwarding-mappings map1;
        no-translation      }
      }
    }
  }
  port-forwarding map1 {
    destined-port 45;
    translated-port 23;
  }
}
```



**NOTE:** Port forwarding and stateful firewall can be configured together. Stateful firewall has precedence over port forwarding.

## Example: Configuring Port Forwarding with Twice NAT

The following example configures port forwarding with **twice-napt-44** as the translation type. The example also has stateful firewall and multiple port maps configured.

```
[edit services]
user@host# show
service-set in {
  syslog {
    host local {
      services any;
    }
  }
  stateful-firewall-rules r;
```

```
    nat-rules r;
    interface-service {
        service-interface sp-10/0/0.0;
    }
}
stateful-firewall {
    rule r {
        match-direction input;
        term t {
            from {
                destination-port {
                    range low 20 high 5000;
                }
            }
            then {
                reject;
            }
        }
    }
}
nat {
    pool x {
        address 12.0.0.2/32;
    }
    rule r {
        match-direction input;
        term t {
            from {
                destination-address {
                    14.0.0.2/32;
                }
                destination-port {
                    range low 10 high 20000;
                }
            }
            then {
                port-forwarding-mappings y;
                translated {
                    destination-pool x;
                    translation-type {
                        twice-napt-44;
                    }
                }
            }
        }
    }
}
port-forwarding y {
    destined-port 45;
    translated-port 23;
    destined-port 55;
    translated-port 33;
    destined-port 65;
    translated-port 43;
}
}
adaptive-services-pics {
    traceoptions {
        file sp-trace;
        flag all;
    }
}
```

**NOTE:**

- Stateful firewall has precedence over port forwarding. In this example, for instance, no traffic destined to any port between 20 and 5000 will be translated.
- Up to 32 port maps can be configured.

**Related Documentation**

- [Configuring Port Forwarding for Static Destination Address Translation on page 251](#)

## Configuring Port Control Protocol

This topic describes the following configuration tasks:

- [Configuring PCP Server Options on page 257](#)
- [Configuring a PCP Rule on page 258](#)
- [Configuring a Service Set to Apply PCP on page 259](#)
- [SYSLOG Message Configuration on page 259](#)

### Configuring PCP Server Options

1. Go to the `[edit services pcp pcp-server server-name]` hierarchy level and specify a PCP server name.

```
user @host# edit services pcp pcp-server server-name
```

2. Set the IPv4 or IPv6 addresses of the server. For PCP DS-Lite, the **ipv6-address** must match the address of the AFTR (Address Family Transition Router or software concentrator).

```
[edit services pcp pcp-server s1]
user @host# set ipv6-address ipv6-address
```

or

```
[edit services pcp pcp-server s1]
user @host# set ipv4-address ipv4-address
```

3. For PCP DS-Lite, provide the name of the DS-Lite software concentrator configuration.

```
[edit services pcp pcp-server s1]
user @host# set software-concentrator software-concentrator-name
```

4. Specify the minimum and maximum mapping lifetimes for the server.

```
[edit services pcp pcp-server s1]
user @host# set mapping-lifetime-minimum mapping-lifetime-minimum
user @host# set mapping-lifetime-maximum mapping-lifetime-maximum
```

5. Specify the time limits for generating short lifetime or long lifetime errors.

```
[edit services pcp pcp-server s1]
user @host# set short-lifetime-error short-lifetime-error
user @host# set long-lifetime-error long-lifetime-error
```

6. (Optional)—Enable PCP options on the specified PCP server. The following options are available—**third-party** and **prefer-failure**. The third-party option is required to enable third-party requests by the PCP client. DS-Lite requires the **third-party** option. The **prefer-failure** option requests generation of an error message when the PCP client requests a specific IP address/port that is not available, rather than assigning another available address from the NAT pool. If **prefer-failure** is not specified NAPT44 assigns an available address/port from the NAT pool based on the configured NAT options.

```
[edit services pcp pcp-server s1]
user @host# set pcp-options third-party
user @host# set pcp-options prefer-failure
```

7. (Optional)—Specify which NAT pool to use for mapping.

```
[edit services pcp pcp-server s1]
user @host# set nat-options pcp-nat-pool pool-name1 <poolname2...>
```

---



**NOTE:** When you do not explicitly specify a NAT pool for mapping, the Junos OS performs a partial rule match based on source IP, source port and protocol; the Junos OS uses the NAT pool configured for the first matching rule to allocate mappings for PCP.

You *must* use explicit configuration in order to use multiple NAT pools.

---

8. (Optional)—Configure the maximum number of mappings per client. The default is 32 and maximum is 128.

```
[edit services pcp pcp-server s1]
user @host# set max-mappings-per-client max-mappings-per-client
```

---

### Configuring a PCP Rule

---

A PCP rule is has the same basic options as all service set rules:

- A **term** option that allows a single rule to have multiple applications.
  - A **from** option that identifies the traffic that is subject to the rule.
  - A **then** option that identifies what action is to be taken. In the case of a PCP rule, this option identifies the pcp server that handles selected traffic
1. Go to the **[edit services pcp rule *rulename*]** hierarchy level and specify **match-direction** input.

```
user @host# edit services pcp rule rulename
user @host# set match-direction input
```
  2. Go to the **[edit services pcp rule *rulename* term *termname*]** hierarchy level and provide a *termname*.

```
user @host# edit term termname
```
  3. (Optional)—Provide a **from** option to filter the traffic to be selected for processing by the rule. When you omit the **from** option, all traffic handled by the service set's service interface is subject to the rule.

4. Set the **then** option to identify the target pcp server.

```
[edit services pcp rule rulename term termname]
user @host# set then pcp-server server-name
```

### Configuring a Service Set to Apply PCP

To use PCP, you must provide the rule-name (or name of a list of rulenames) in the **pcp-rule *rulename*** option.

1. Go to the **[edit services service-set *service-set-name*** hierarchy level.

```
user @host# edit services service-set service-set-name
```

2. If this is a new service set, provide basic service set information, including interface information and any other rules that may apply.
3. Specify the name of the PCP rule or rule list used to send traffic to the specified PCP server.

```
[edit services service-set service-set-name ]
user @host# set pcp-rule rule-name | rule-listname
```



**NOTE:** Your service set must also identify any required **nat-rule** and **software-rule**.

### SYSLOG Message Configuration

A new syslog class, configuration option, **pcp-logs**, has been provided to control PCP log generation. It provides the following levels of logging:

- **protocol**—All logs related to mapping creation, deletion are included at this level of logging.
- **protocol-error**—All protocol error related logs (such as mapping refresh failed, PCP look up failed, mapping creation failed). are included in this level of logging.
- **system-error**—Memory and infrastructure errors are included in this level of logging.

## Example: NAT 44 CGN Configurations

This example describes how to implement several NAT configurations.

- [Hardware and Software Requirements on page 260](#)
- [Overview on page 260](#)
- [Basic NAT44 Configuration on page 260](#)

## Hardware and Software Requirements

This example requires the following hardware:

- An MX Series 3D Universal Edge router with a Services DPC or an M Series Multiservice Edge router with a services PIC
- A domain name server (DNS)

This example uses the following software:

- Junos OS Release 11.4 or higher

## Overview

This example shows a complete CGN NAT44 configuration and advanced options.

## Basic NAT44 Configuration

---

### Chassis Configuration

#### Step-by-Step Procedure

To configure the service PIC (FPC 5 Slot 0) with the Layer 3 service package:

1. Go to the **[edit chassis]** hierarchy level.

```
user@host# edit chassis
```

2. Configure the Layer 3 service package.

```
[edit chassis]
```

```
user@host# set fpc 5 pic 0 adaptive-services service-package layer-3
```

---

### Configuring the Interfaces

#### Step-by-Step Procedure

To configure interfaces to the private network and the public Internet:

1. Define the interface to the private network.

```
user@host# edit interfaces ge-1/3/5
```

```
[edit interfaces ge-1/3/5]
```

```
user@host# set description "Private"
```

```
user@host# edit unit 0 family inet
```

```
[edit interfaces ge-1/3/5 unit 0 family inet]
```

```
user@host# set service input service-set ss2
```

```
user@host# set service output service-set ss2
```

```
user@host# set address 9.0.0.1/24
```

2. Define the interface to the public Internet.

```
user@host# edit interfaces ge-1/3/6
```

```
[edit interfaces ge-1/3/6]
```

```
user@host# set description "Public"
```

```
user@host# set unit 0 family inet address 128.0.0.1/24
```

3. Define the service interface for NAT processing.

```
user@host# edit interfaces sp-5/0/0
```

```
[edit interfaces sp-5/0/0]
user@host# set unit 0 family inet
```

**Results**

```
user@host# show interfaces ge-1/3/5
description Private;
unit 0 {
  family inet {
    service {
      input {
        service-set sset2;
      }
      output {
        service-set sset2;
      }
    }
    address 9.0.0.1/24;
  }
}
```

```
user@host# show interfaces ge-1/3/6
description Public;;
unit 0 {
  family inet {
    address 128.0.0.1/24;
  }
}
```

```
user@host# show interfaces sp-5/0/0
unit 0 {
  family inet;
}
```

### Configuring NAT with Port Translation

**Step-by-Step Procedure** To configure source-only dynamic NAT with port translation:

1. Configure the NAT pool.
 

```
user@host# edit services nat
[edit services nat]
user@host# set pool p1 address 129.0.0.0/24
user@host# set pool p1 port automatic random-allocation
```
2. Configure the NAT rule.
 

```
[edit services nat]
host# edit rule r1
host# set match-direction input
host# set term t1 from source-address 10.0.0.0/16
host# set term t1 from source-address 10.1.0.0/16
host# set term t1 then translated source-pool p1 translation-type dynamic-nat44
```

**Results**    `user@host# show services nat`

```
pool p1 {
  address 129.0.0.0/24;
}
rule r1 {
  match-direction input;
  term t1 {
    from {
      source-address {
        10.0.0.0/16;
        10.1.0.0/16;
      }
    }
    then {
      translated {
        source-pool p1;
        translation-type {
          dynamic-nat44;
        }
      }
    }
  }
}
```

---

### Configuring the Service Set

---

#### Step-by-Step Procedure

To configure the service set:

1. Configure a service set.

```
user@host# edit services service-set ss2
```

2. Specify the NAT rule to be used.

```
[edit services service-set ss2]
host# set nat-rules r1
```

3. Specify the interface service.

```
[edit services service-set ss2]
host# set interface-service service-interface sp-5/0/0
```

**Results** `user@host# show services service-sets sset2`

```
nat-rules r1;
interface-service {
    service-interface sp-5/0/0;
}
```

## Example: NAPT Configuration for the MS-MPC

This example shows how to configure network address translation with port translation (NAPT) on an MX series router using a MultiServices Modular Port Concentrator (MS-MPC) as a services interface card.

- [Requirements on page 263](#)
- [Overview on page 263](#)
- [Configuration on page 263](#)

### Requirements

This example uses the following hardware and software components:

- MX-series router
- MultiServices Modular Port Concentrator (MS-MPC)
- Junos OS Release 13.2R1 or higher

### Overview

A service provider has chosen an MS-MPC as a platform to provide NAT services to accommodate new subscribers.

### Configuration

To configure NAPT<sup>44</sup> using the MS-MPC as a services interface card, perform these tasks:

- [Configuring Interfaces on page 264](#)
- [Configure an Application Set of Acceptable ALG traffic on page 265](#)
- [Configuring a Stateful Firewall Rule on page 265](#)
- [Configuring NAT Pool and Rule on page 266](#)
- [Configuring the Service Set on page 267](#)

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set interfaces ge-0/2/0 unit 0 family inet address 10.255.248.2/24
set interfaces xe-1/1/0 unit 0 family inet address 10.255.247.2/24
set interfaces xe-1/1/0 unit 0 family inet service input service-set sset1
set interfaces xe-1/1/0 unit 0 family inet service output service-set sset1
```

```

set interfaces ms-3/0/0 unit 0 family inet
set applications application-set accept-algs application junos-http
set applications application-set accept-algs application junos-ftp
set applications application-set accept-algs application junos-tftp
set applications application-set accept-algs application junos-telnet
set applications application-set accept-algs application junos-sip
set applications application-set accept-algs application junos-rtcp
set services stateful-firewall rule sf-rule1 match-direction input-output
set services stateful-firewall rule sf-rule1 term sf-term1 from source-address
    10.255.247.0/24
set services stateful-firewall rule sf-rule1 term sf-term1 from application-sets accept-algs
set services stateful-firewall rule sf-rule1 term sf-term1 then accept
set services nat pool napt-pool address 1.1.1.0/24
set services nat pool napt-pool port automatic
* nat rule for napt
set services nat rule nat-rule1 match-direction input
set services nat rule nat-rule1 term nat-term1 from source-address 10.255.247.0/24
set services nat rule nat-rule1 term nat-term1 from application-sets accept-algs
set services nat rule nat-rule1 term nat-term1 then translated source-pool napt-pool
set services nat rule nat-rule1 term nat-term1 then translated translation-type napt-44
* nat rule for basic nat
set services service-set sset1 stateful-firewall-rules sf-rule1
set services service-set sset1 nat-rules nat-rule1
set services service-set sset1 interface-service service-interface ms-3/0/0

```

## Configuring Interfaces

### Step-by-Step Procedure

Configure the interfaces required for NAT processing. You will need the following interfaces:

- A customer-facing interface that handles traffic from and to the customer.
- An internet-facing interface.
- A services interface that provides NAT and stateful firewall services to the customer-facing interface

1. Configure the interface for the customer-facing interface.

```

user@host# edit
[edit ]
user@host# set interfaces xe-1/1/0 unit 0 family inet address 10.255.247.2/24
user@host# set interfaces xe-1/1/0 unit 0 family inet service input service-set sset1
user@host# set interfaces xe-1/1/0 unit 0 family inet service output service-set sset1

```

2. Configure the interface for the Internet-facing interface.

```

[edit ]
set interfaces ge-0/2/0 unit 0 family inet address 10.255.248.2/24

```

3. Configure the interface for the service set that will connect services to the customer-facing interface. In our example, the interface resides on an MS-MPC.

```

[edit ]
user@host# set interfaces ms-3/0/0 unit 0 family inet

```

### Configure an Application Set of Acceptable ALG traffic

<b>Step-by-Step Procedure</b>	<p>Identify the acceptable ALGs for incoming traffic.</p> <ol style="list-style-type: none"> <li>Specify an application set that contains acceptable incoming ALG traffic.           <pre> user@host# set applications application-set accept-algs application junos-http user@host# set applications application-set accept-algs application junos-ftp user@host# set applications application-set accept-algs application junos-tftp user@host# set applications application-set accept-algs application junos-telnet user@host# set applications application-set accept-algs application junos-sip user@host# set applications application-set accept-algs application junos-rtcp </pre> </li> </ol>
<b>Results</b>	<pre> user@host#edit services applications application-set accept-algs user@host#show application junos-http; application junos-ftp; application junos-tftp; application junos-telnet; application junos-sip; application junos- </pre>

### Configuring a Stateful Firewall Rule

<b>Step-by-Step Procedure</b>	<p>Configure a stateful firewall rule that will accept all incoming traffic.</p> <ol style="list-style-type: none"> <li>Specify firewall matching for all input and output           <pre> user@host# set services stateful-firewall rule sf-rule1 match-direction input-output </pre> </li> <li>Identify source-address and acceptable ALG traffic from the customer-facing interface.           <pre> user@host# set services stateful-firewall rule sf-rule1 term sf-term1 from source-address 10.255.247.0/24 user@host# set services stateful-firewall rule sf-rule1 term sf-term1 from application-sets accept-algs user@host# set services stateful-firewall rule sf-rule1 term sf-term1 then accept </pre> </li> </ol>
-------------------------------	--

**Results**

```
user@host# edit services stateful-firewall
user@host# show
rule sf-rule1 {
  match-direction input-output;
  term sf-term1 {
    from {
      source-address {
        10.255.247.0/24;
      }
      application-sets accept-algs;
    }
    then {
      accept;
    }
  }
}
```

---

### Configuring NAT Pool and Rule

---

**Step-by-Step Procedure** Configure a NAT pool and rule for address translation with automatic port assignment.

1. Configure the NAT pool with automatic port assignment.

```
user@host# set services nat pool napt-pool address 1.1.1.0/24
user@host# set services nat pool napt-pool port automatic
```

2. Configure a NAT rule that applies translation type **napt-44** using the defined NAT pool.

```
user@host# set services nat rule nat-rule1 term nat-term1 from application-sets
accept-algs
user@host# set services nat rule nat-rule1 term nat-term1 then translated source-pool
napt-pool
user@host# set services nat rule nat-rule1 term nat-term1 then translated
translation-type napt-44
```

**Results**

```

user@host#edit services nat
user@host#show

pool napt-pool {
    address 1.1.1.0/24;
    port {
        automatic;
    }
}
rule nat-rule1 {
    match-direction input;
    term nat-term1 {
        from {
            source-address {
                10.255.247.0/24;
            }
            application-sets accept-algs;
        }
        then {
            translated {
                source-pool napt-pool;
                translation-type {
                    napt-44;
                }
            }
        }
    }
}

```

### Configuring the Service Set

**Step-by-Step Procedure** Configure an interface type service set.

1. Specify the NAT and stateful firewall rules that apply to customer traffic.
 

```

user@host set services service-set sset1 stateful-firewall-rules sf-rule1
user@host set services service-set sset1 nat-rules bat-rule1

```
2. Specify the services interface that applies the rules to customer traffic.
 

```

set services service-set sset1 interface-service service-interface ms-3/0/0

```

**Results**

```

user@host# edit services service-set sset1
user@host# show
set services service-set sset1 stateful-firewall-rules sf-rule1
set services service-set sset1 nat-rules nat-rule1
set services service-set sset1 interface-service service-interface ms-3/0/0

```

**Related Documentation**

- [Network Address Translation Overview for MS-DPC, MS-MPC, and MS-MIC Line Cards on page 54](#)

## Example: Configuring NAT-PT

A Domain Name System application-level gateway (DNS ALG) is used with Network Address Translation-Protocol Translation (NAT-PT) to facilitate name-to-address

mapping. You can configure the DNS ALG to map addresses returned in the DNS response to an IPv6 address.

When you configure NAT-PT with DNS ALG support, you must configure two NAT rules or one rule with two terms. In this example, you configure two rules. The first NAT rule ensures that the DNS query and response packets are translated correctly. For this rule to work, you must configure a DNS ALG application and reference it in the rule. The second rule is required to ensure that NAT sessions are destined to the address mapped by the DNS ALG.

Then, you must configure a service set, and then apply the service set to the interfaces.

This example describes how to configure NAT-PAT with DNS ALG:

- [Requirements on page 268](#)
- [Overview and Topology on page 268](#)
- [Configuration of NAT-PT with DNS ALGs on page 270](#)

## Requirements

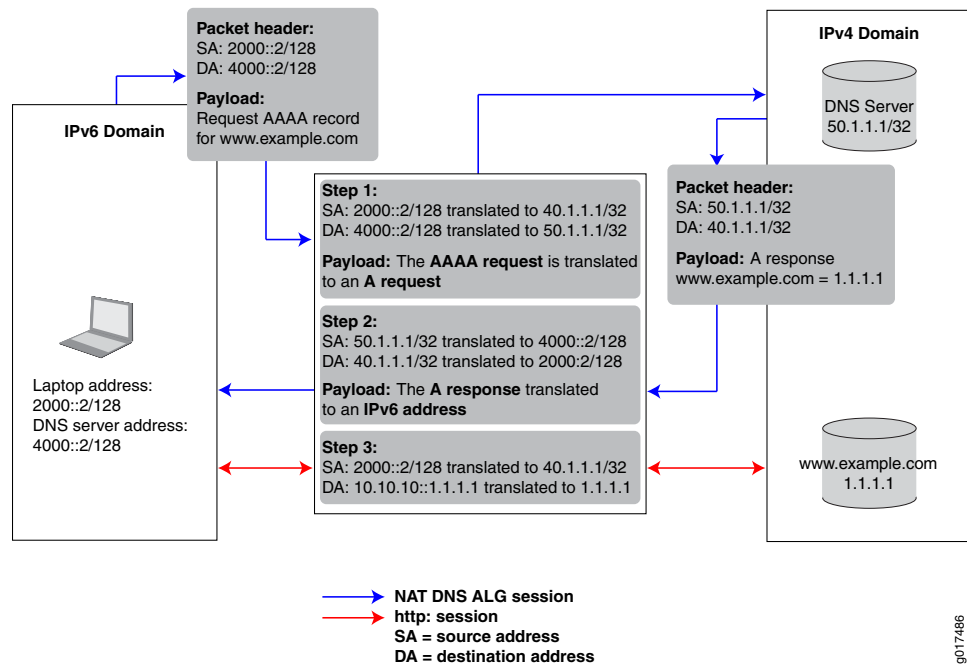
This example uses the following hardware and software components:

- Junos OS Release 11.2
- A multiservices interface (**ms-**)

## Overview and Topology

The following scenario shows the process of NAT-PT with DNS ALG when a laptop in an IPv6-only domain requests access to a server in an IPv4-only domain.

Figure 13: Configuring DNS ALGs with NAT-PT Network Topology



The Juniper Networks router in the center of the illustration performs address translation in two steps. When the laptop requests a session with the **www.example.com** server that is in an IPv4-only domain, the Juniper Networks router performs the following:

- Translates the IPv6 laptop and DNS server addresses into IPv4 addresses.
- Translates the AAAA request from the laptop into an A request so that the DNS server can provide the IPv4 address.

When the DNS server responds with the A request, the Juniper Networks router performs the following:

- Translates the IPv4 DNS server address back into an IPv6 address.
- Translates the A request back into a AAAA request so that the laptop now has the 96-bit IPv6 address of the **www.example.com** server.

After the laptop receives the IPv6 version of the **www.example.com** server address, the laptop initiates a second session using the 96-bit IPv6 address to access that server. The Juniper Networks router performs the following:

- Translates the laptop IPv4 address directly into its IPv4 address.
- Translates the 96-bit IPv6 **www.example.com** server address into its IPv4 address.

## Configuration of NAT-PT with DNS ALGs

To configure NAT-PT with DNS ALG, perform the following tasks:

- [Configuring the Application-Level Gateway on page 270](#)
- [Configuring the NAT Pools on page 271](#)
- [Configuring the DNS Server Session: First NAT Rule on page 272](#)
- [Configuring the HTTP Session: Second NAT Rule on page 275](#)
- [Configuring the Service Set on page 277](#)
- [Configuring the Stateful Firewall Rule on page 279](#)
- [Configuring Interfaces on page 280](#)

---

### Configuring the Application-Level Gateway

#### Step-by-Step Procedure

Configure the DNS application as the ALG to which the DNS traffic is destined. The DNS application protocol closes the DNS flow as soon as the DNS response is received. When you configure the DNS application protocol, you must specify the UDP protocol as the network protocol to match in the application definition.

To configure the DNS application:

1. In configuration mode, go to the **[edit applications]** hierarchy level.

```
user@host# edit applications
```

2. Define the application name and specify the application protocol to use in match conditions in the first NAT rule.

```
[edit applications]
user@host# set application application-name application-protocol protocol-name
```

For example:

```
[edit applications]
user@host# set application dns_alg application-protocol dns
```

3. Specify the protocol to match, in this case UDP.

```
[edit applications]
user@host# set application application-name protocol type
```

For example:

```
[edit applications]
user@host# set application dns_alg protocol udp
```

4. Define the UDP destination port for additional packet matching, in this case the domain port.

```
[edit applications]
user@host# set application application-name destination-port value
```

For example:

```
[edit applications]
user@host# set application dns_alg destination-port 53
```

**Results** [edit applications]  
 user@host# show  
 application dns\_alg {  
   application-protocol dns;  
   protocol udp;  
   destination-port 53;  
 }

### Configuring the NAT Pools

**Step-by-Step Procedure** In this configuration, you configure two pools that define the addresses (or prefixes) used for NAT. These pools define the IPv4 addresses that are translated into IPv6 addresses. The first pool includes the IPv4 address of the source. The second pool defines the IPv4 address of the DNS server. To configure NAT pools:

1. In configuration mode, go to the **[edit services nat]** hierarchy level.  
 user@host# edit services nat
2. Specify the name of the first pool and the IPv4 source address (laptop).  
 [edit services nat]  
 user@host# set pool *nat-pool-name* address *ip-prefix*

For example:

```
[edit services nat]
user@host# set pool pool1 address 40.1.1.1/32
```

3. Specify the name of the second pool and the IPv4 address of the DNS server.  
 [edit services nat]  
 user@host# set pool *nat-pool-name* address *ip-prefix*

For example:

```
[edit services nat]
user@host# set pool pool2 address 50.1.1.1/32
```

**Results** The following sample output shows the configuration of NAT pools.

```
[edit services nat]
user@host# show
pool pool1 {
  address 40.1.1.1/32;
}
pool pool2 {
  address 50.1.1.1/32;
}
```

### Configuring the DNS Server Session: First NAT Rule

---

**Step-by-Step Procedure** The first NAT rule is applied to DNS traffic going to the DNS server. This rule ensures that the DNS query and response packets are translated correctly. For this rule to work, you must configure a DNS ALG application and reference it in the rule. The DNS application was configured in [“Configuring the DNS ALG Application” on page 240](#). In addition, you must specify the direction in which traffic is matched, the source address of the laptop, the destination address of the DNS server, and the actions to take when the match conditions are met.

To configure the first NAT rule:

1. In configuration mode, go to the **[edit services nat]** hierarchy level.

```
user@host# edit services nat
```

2. Specify the name of the NAT rule.

```
[edit services nat]
user@host# edit rule rule-name
```

For example:

```
[edit services nat]
user@host# edit rule rule1
```

3. Specify the name of the NAT term.

```
[edit services nat rule rule-name]
user@host# edit term term-name
```

For example:

```
[edit services nat rule rule1]
user@host# edit term term1
```

4. Define the match conditions for this rule.
  - a. Specify the IPv6 source address of the device (laptop) attempting to access an IPv4 address.

```
[edit services nat rule rule-name term term-name]
user@host# set from source-address source-address
```

For example:

```
[edit services nat rule rule1 term term1]
user@host# set from source-address 2000::2/128
```

- b. Specify the IPv6 destination address of the DNS server.

```
[edit services nat rule rule-name term term-name]
user@host# set from destination-address prefix
```

For example:

```
[edit services nat rule rule1 term term1]
user@host# set from destination-address 4000::2/128
```

- c. Reference the DNS application to which the DNS traffic destined for port 53 is applied.

```
[edit services nat rule rule1 term term1]
user@host# set from applications application-name
```

In this example, the application name configured in the *Configuring the DNS Application* step is `dns_alg`:

```
[edit services nat rule rule1 term term1]
user@host# set from applications dns_alg
```

5. Define the actions to take when the match conditions are met. The source and destination pools you configured in “[Configuring the NAT Pools](#)” on page 271 are applied here.

- a. Apply the NAT pool configured for source translation.

```
[edit services nat rule rule-name term term-name]
user@host# set then translated source-pool nat-pool-name
```

For example:

```
[edit services nat rule rule1 term term1]
user@host# set then translated source-pool pool1
```

- b. Apply the NAT pool configured for destination translation.

```
[edit services nat rule rule-name term term-name]
user@host# set then translated destination-pool nat-pool-name
```

For example:

```
[edit services nat rule rule1 term term1]
user@host# set then translated source-pool pool2
```

6. Define the DNS ALG 96-bit prefix for IPv4-to-IPv6 address mapping.

```
[edit services nat rule rule-name term term-name]
user@host# set then translated dns-alg-prefix dns-alg-prefix
```

For example:

```
[edit services nat rule rule1 term term1]
user@host# set then translated dns-alg-prefix 10:10:10::0/96
```

7. Specify the type of NAT used for source and destination traffic.

```
[edit services nat rule rule-name term term-name]
user@host# set then translated translation-type basic-nat-pt
```

For example:

```
[edit services nat rule rule1 term term1]
user@host# set then translated translation-type basic-nat-pt
```



**NOTE:** In this example, since NAT is achieved using address-only translation, the `basic-nat-pt` translation type is used. To achieve NAT using address and port translation (NAPT), use the `napt-pt` translation type.

8. Specify the direction in which to match traffic that meets the rule conditions.

```
[edit services nat rule rule-name]  
user@host# set match-direction (input | output)
```

For example:

```
[edit services nat rule rule1]  
user@host# set match-direction input
```

9. Configure system logging to record information from the services interface to the /var/log directory.

```
[edit services nat rule rule-name term term-name]  
user@host# set then syslog
```

For example:

```
[edit services nat rule rule1 term term1]  
user@host# set then syslog
```

**Results** The following sample output shows the configuration of the first NAT rule that goes to the DNS server.

```
[edit services nat]
user@host# show
rule rule1 {
  match-direction input;
  term term1 {
    from {
      source-address {
        2000::2/128;
      }
      destination-address {
        4000::2/128;
      }
      applications dns_alg;
    }
    then {
      translated {
        source-pool pool1;
        destination-pool pool2;
        dns-alg-prefix 10:10:10::0/96;
        translation-type {
          basic-nat-pt;
        }
      }
      syslog;
    }
  }
}
```

### Configuring the HTTP Session: Second NAT Rule

**Step-by-Step Procedure** The second NAT rule is applied to destination traffic going to the IPv4 server ([www.example.com](http://www.example.com)). This rule ensures that NAT sessions are destined to the address mapped by the DNS ALG. For this rule to work, you must configure the DNS ALG address map that correlates the DNS query or response processing done by the first rule with the actual data sessions processed by the second rule. In addition, you must specify the direction in which traffic is matched: the IPv4 address for the IPv6 source address (laptop), the 96-bit prefix to prepend to the IPv4 destination address ([www.example.com](http://www.example.com)), and the translation type.

To configure the second NAT rule:

1. In configuration mode, go to the following hierarchy level.

```
user@host# edit services nat
```

2. Specify the name of the NAT rule and term.

```
[edit services nat]
user@host# edit rule rule-name term term-name
```

For example:

```
[edit services nat]
user@host# edit rule rule2 term term1
```

3. Define the match conditions for this rule:
  - a. Specify the IPv6 address of the device attempting to access the IPv4 server.

```
[edit services nat rule rule-name term term-name]  
user@host# set from source-address source-address
```

For example:

```
[edit services nat rule rule2 term term1]  
user@host# set from source-address 2000::2/128
```

- b. Specify the 96-bit IPv6 prefix to prepend to the IPv4 server address.

```
[edit services nat rule rule-name term term-name]  
user@host# set from destination-address prefix
```

For example:

```
[edit services nat rule rule2 term term1]  
user@host# set from destination-address 10:10:10::c0a8:108/128
```

4. Define the actions to take when the match conditions are met.
  - Specify the prefix for the translation of the IPv6 source address.

```
[edit services nat rule rule-name term term-name]  
user@host# set then translated source-prefix source-prefix
```

For example:

```
[edit services nat rule rule2 term term1]  
user@host# set then translated source-prefix 19.19.19.1/32
```

5. Specify the type of NAT used for source and destination traffic.

```
[edit services nat rule rule-name term term-name]  
user@host# set then translated translation-type basic-nat-pt
```

For example:

```
[edit services nat rule rule2 term term1]  
user@host# set then translated translation-type basic-nat-pt
```



**NOTE:** In this example, since NAT is achieved using address-only translation, the **basic-nat-pt** translation type is used. To achieve NAT using address and port translation (NAPT), you must use the **napt-pt** translation type.

---

6. Specify the direction in which to match traffic that meets the conditions in the rule.

```
[edit services nat rule rule-name]  
user@host# set match-direction (input | output)
```

For example:

```
[edit services nat rule rule2]  
user@host# set match-direction input
```

**Results** The following sample output shows the configuration of the second NAT rule.

```
[edit services nat]
user@host# show
rule rule2 {
  match-direction input;
  term term1 {
    from {
      source-address {
        2000::2/128;
      }
      destination-address {
        10:10:10::c0a8:108/128;
      }
    }
    then {
      translated {
        source-prefix 19.19.19.1/32;
        translation-type {
          basic-nat-pt;
        }
      }
    }
  }
}
```

### Configuring the Service Set

**Step-by-Step Procedure** This service set is an interface service set used as an action modifier across the entire services (**ms-**) interface. Stateful firewall and NAT rule sets are applied to traffic processed by the services interface.

To configure the service set:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```
user@host# edit services
```

2. Define a service set.

```
[edit services]
user@host# edit service-set service-set-name
```

For example:

```
[edit services]
user@host# edit service-set ss
```

3. Specify properties that control how system log messages are generated for the service set.

```
[edit services service-set ss]
user@host# set syslog host local services severity-level
```

The example below includes all severity levels.

```
[edit services service-set ss]
user@host# set syslog host local services any
```

4. Specify the stateful firewall rule included in this service set.

```
[edit services service-set ss]
user@host# set stateful-firewall-rules rule1 severity-level
```

The example below references the stateful firewall rule defined in [“Configuring the Stateful Firewall Rule” on page 279](#).

```
[edit services service-set ss]
user@host# set stateful-firewall-rules rule1
```

5. Define the NAT rules included in this service set.

```
[edit services service-set ss]
user@host# set nat-rules rule-name
```

The example below references the two rules defined in this configuration example.

```
[edit services service-set ss]
user@host# set nat-rules rule1
user@host# set nat-rules rule2
```

6. Configure an adaptive services interface on which the service is to be performed.

```
[edit services service-set ss]
user@host# set interface-service service-interface interface-name
```

For example:

```
[edit services service-set ss]
user@host# interface-service service-interface ms-2/0/0
```

Only the device name is needed, because the router software manages logical unit numbers automatically. The services interface must be an adaptive services interface for which you have configured **unit 0 family inet** at the `[edit interfaces interface-name]` hierarchy level in [“Configuring Interfaces” on page 280](#).

**Results** The following sample output shows the configuration of the service set.

```
[edit services]
user@host# show
service-set ss {
  syslog {
    host local {
      services any;
    }
  }
  stateful-firewall-rules rule1;
  nat-rules rule1;
  nat-rules rule2;
  interface-service {
    service-interface ms-2/0/0;
  }
}
```

### Configuring the Stateful Firewall Rule

**Step-by-Step Procedure** This example uses a stateful firewall to inspect packets for state information derived from past communications and other applications. The NAT-PT router checks the traffic flow matching the direction specified by the rule, in this case both input and output. When a packet is sent to the services (**ms-**) interface, direction information is carried along with it.

To configure the stateful firewall rule:

1. In configuration mode, go to the **[edit services stateful firewall]** hierarchy level.

```
user@host# edit services stateful firewall
```

2. Specify the name of the stateful firewall rule.

```
[edit services stateful-firewall]
user@host# edit rule rule-name
```

For example:

```
[edit services stateful-firewall]
user@host# edit rule rule1
```

3. Specify the direction in which traffic is to be matched.

```
[edit services stateful-firewall rule rule-name]
user@host# set match-direction (input | input-output | output)
```

For example:

```
[edit services stateful-firewall rule rule1]
user@host# set match-direction input-output
```

4. Specify the name of the stateful firewall term.

```
[edit services stateful-firewall rule rule-name]
user@host# edit term term-name
```

For example:

```
[edit services stateful-firewall rule rule1]
user@host# edit term term1
```

5. Define the terms that make up this rule.

```
[edit services stateful-firewall rule rule-name term term-name]  
user@host# set then accept
```

For example:

```
[edit services stateful-firewall rule rule1 term term1]  
user@host# set then accept
```

**Results** The following sample output shows the configuration of the services stateful firewall.

```
[edit services]  
user@host# show  
stateful-firewall {  
  rule rule1 {  
    match-direction input-output;  
    term term1 {  
      then {  
        accept;  
      }  
    }  
  }  
}
```

---

### Configuring Interfaces

**Step-by-Step Procedure** After you have defined the service set, you must apply services to one or more interfaces installed on the router. In this example, you configure one interface on which you apply the service set for input and output traffic. When you apply the service set to an interface, it automatically ensures that packets are directed to the services (**ms-**) interface.

To configure the interfaces:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level.

```
user@host# edit interfaces
```

2. Configure the interface on which the service set is applied to automatically ensure that packets are directed to the services (**ms-**) interface.

- a. For IPv4 traffic, specify the IPv4 address.

```
[edit interfaces]  
user@host# set ge-1/0/9 unit 0 family inet address 30.1.1.1/24
```

- b. Apply the service set defined in [“Configuring Interfaces” on page 280](#).

```
[edit interfaces]  
user@host# set ge-1/0/9 unit 0 family inet6 service input service-set ss  
user@host# set ge-1/0/9 unit 0 family inet6 service output service-set ss
```

- c. For IPv6 traffic, specify the IPv6 address.

```
[edit interfaces]  
user@host# set ge-1/0/9 unit 0 family inet6 address 2000::1/64
```

3. Specify the interface properties for the services interface that performs the service.

```
[edit interfaces]
user@host# set ms-2/0/0 services-options syslog host local services any
user@host# set ms-2/0/0 unit 0 family inet
user@host# set ms-2/0/0 unit 0 family inet6
```

**Results** The following sample output shows the configuration of the interfaces for this example.

```
[edit interfaces]
user@host# show

ge-1/0/9 {
  unit 0 {
    family inet {
      address 30.1.1.1/24;
    }
    family inet6 {
      service {
        input {
          service-set ss;
        }
        output {
          service-set ss;
        }
      }
      address 2000::1/64;
    }
  }
}

ms-2/0/0 {
  services-options {
    syslog {
      host local {
        services any;
      }
    }
  }
  unit 0 {
    family inet;
    family inet6;
  }
}
```

- Related Documentation**
- [Network Address Translation Overview for MS-DPC, MS-MPC, and MS-MIC Line Cards on page 54](#)
  - [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)
  - [Example: Configuring Layer 3 Services and the Services SDK on Two PICs](#)
  - [dns-alg-prefix on page 316](#)
  - [dns-alg-pool on page 316](#)

## Example: Configuring Inline Network Address Translation - Interface-Service Service Set

---

- [Requirements on page 282](#)
- [Overview on page 282](#)
- [Configuration on page 284](#)

### Requirements

This example uses the following hardware and software components:

- MX-series router
- MultiServices Dense Port Concentrator (MS-DPC)
- Junos OS Release 11.4R1 or higher

### Overview

This example is configured for the network of a large financial services firm. This Application Service Provider (ASP) has an IP/MPLS-based backbone and provides L3VPN connectivity. In our example, the ASP acts like an Internet Service Provider (ISP) and its servers have public IPv4 addresses.

A large subscriber base relies heavily on the market data feeds that the ASP provides. Like many of the enterprise networks today, a private addressing scheme has been in place for majority of ASP's customers. NAT is required to maintain access to ASP's shared services.

Requirements for the solution include:

- Ease subscriber addressing challenges of their by providing NAT services in ASP's network.
- Support access to common services by a large number of customers, even when these are hosted across in different VRFs and use overlapping addresses.
- Provide high throughput, low latency packet forwarding with NAT enabled.
- Provide operational simplicity and efficiency.
- Reduce cost of operations.

By deploying Juniper's MX's inline NAT service, the ASP can offer scalable solutions with uncompromised performance that fit the requirements of financial markets customers. Operational cost can be dramatically reduced by eliminating the need for a dedicated services PIC. Enabling subscribers to keep their existing addressing scheme by outsourcing the address translation function to the ASP greatly simplifies their network operations.

### Topology

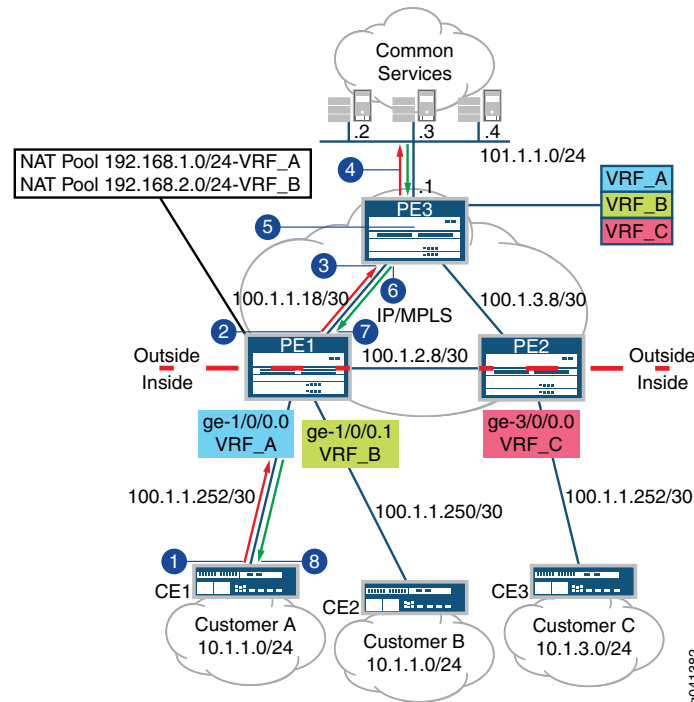
---

The topology for this application is show in [Figure 14 on page 283](#)

The ASP's shared services are located on LAN segment 101.1.1.0/24 behind PE3. PE1 and PE2 are used to connect subscribers. Traditional MPLS-VPN is deployed between provider edge routers. In the case of PE1, subscriber A and B have overlapping addressing schemes of 10.1.1.0/24; NAT is needed so the subscribers can access the same server. NAT pools 192.168.1.0/24 and 192.168.2.0/24 have been allocated to customer A and B respectively.

We will use host 10.1.1.2 from customer A to illustrate packet flow at a high level, as shown in Figure 14 on page 283

Figure 14: Deploy Inline NAT within L3VPN



1. CE1 forwards request from host 10.1.1.2 with a server destination of 101.1.1.2
2. With configured service set on PE1 for VRF\_A, source address of 10.1.1.2 will be translated into 192.168.1.2. VPN label and IGP label will be imposed after the translation.
3. Packets will then be forwarded to PE3 using IGP label
4. PE3 receives the packet and performs a lookup in its VPN routing table. It then forwards the packets to server 101.1.1.2 after label disposition.
5. The server returns the packet with destination address of 192.168.1.2.
6. PE3 imposes VPN and IGP labels for the above destination and label switched the packets to PE1.
7. PE1 sends the packet to VRF\_A after a FIB lookup. Destination address 192.168.1.2 will be translated 10.1.1.2.
8. CE1 receives the packets for host 10.1.1.2 and forwards them on.

## Configuration

By using a **si-** (service-inline) interface, the operator can configure both **interface-service** and **next-hop** service-sets to perform inline NAT. This example uses the **interface-service** service set.

To configure inline NAT, perform these tasks:

- [Configure Interfaces on page 284](#)
- [Configuring Bandwidth for the Service Inline \(si-\) Interface on page 286](#)
- [Configuring NAT Pool and Rule on page 287](#)
- [Configuring the Service Set on page 289](#)

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set interfaces si-0/0/0 unit 0 family inet
set interfaces ge-1/0/0 unit 0 family inet service input service-set nat1
set interfaces ge-1/0/0 unit 0 family inet service output service-set nat1
set interfaces ge-1/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces ge-1/0/1 unit 0 family inet service input service-set nat2
set interfaces ge-1/0/1 unit 0 family inet service output service-set nat2
set interfaces ge-1/0/1 unit 0 family inet address 192.168.1.1/24
set interfaces ge-1/0/2 unit 0 family inet service input service-set nat3
set interfaces ge-1/0/2 unit 0 family inet service output service-set nat3
set interfaces ge-1/0/2 unit 0 family inet address 10.1.1.100/24
set chassis fpc 0 pic 0 inline-services bandwidth 10g
set services nat pool p1 address 20.1.1.0/24
set services nat pool p2 address 21.1.1.2/32
set services nat pool p3 address 120.1.1.1/32
set services nat rule r1 match-direction input
set services nat rule r1 term t1 from source-address 10.1.1.0/24
set services nat rule r1 term t1 then translated source-pool p1 translation-type basic-nat44
set services nat rule r2 match-direction input
set services nat rule r2 term t1 from source-address 192.168.1.2/32
set services nat rule r2 term t1 then translated source-pool p2 translation-type basic-nat44
set services nat rule r3 match-direction input
set services nat rule r3 term t1 from source-address 10.1.1.8/32
set services nat rule r3 term t1 then translated source-pool p3 translation-type basic-nat44
set services service-set nat1 nat-rules r1
set services service-set nat1 interface-service service-interface si-0/0/0.0
set services service-set nat2 nat-rules r2
set services service-set nat2 interface-service service-interface si-0/0/0.0
set services service-set nat3 nat-rules r3
```

---

### Configure Interfaces

#### Step-by-Step Procedure

To configure interfaces required for inline NAT:

1. Configure the inline interface for NAT services.

```
user@host# edit interfaces si-0/0/0
[edit interfaces si-0/0/0]
user@host# set unit 0 family inet
```

2. Configure the interface for traffic to be handled by service set nat1

```
user@host# edit interfaces ge-1/0/0
[edit interfaces ge-1/0/0]
user@host# edit unit 0 family inet service
[edit unit 0 family inet service]
user@host# set input service-set nat1 output service-set nat1
user@host# set address 10.1.1/24
```

3. Configure the interface for traffic to be handled by service set nat2

```
user@host# edit interfaces ge-1/0/1
[edit interfaces ge-1/0/0]
user@host# edit unit 0 family inet service input service
[edit unit 0 family inet service]
user@host# set input service-set nat2 output service-set nat2
user@host# set address 192.168.1/24
```

4. Configure the interface for traffic to be handled by service set nat3

```
user@host# edit interfaces ge-1/0/2
[edit interfaces ge-1/0/0]
user@host# edit unit 0 family inet service input service
[edit unit 0 family inet service]
user@host# set input service-set nat3 output service-set nat3
user@host# set address 10.1.1.100/24
```

```

Results  si-0/0/0 {
          unit 0 {
            family inet;
          }
        }
        ge-1/0/0 {
          unit 0 {
            family inet {
              service {
                input {
                  service-set nat1;
                }
                output {
                  service-set nat1;
                }
              }
            }
            address 10.1.1.1/24;
          }
        }
        ge-1/0/1 {
          unit 0 {
            family inet {
              service {
                input {
                  service-set nat2;
                }
                output {
                  service-set nat2;
                }
              }
            }
            address 192.168.1.1/24;
          }
        }
        ge-1/0/2 {
          unit 0 {
            family inet {
              service {
                input {
                  service-set nat3;
                }
                output {
                  service-set nat3;
                }
              }
            }
            address 10.1.1.1/24;
          }
        }
      }

```

### Configuring Bandwidth for the Service Inline (si-) Interface

#### Step-by-Step Procedure

1. Go to the configuration hierarchy for the fpc and pic used for inline NAT services.  

```

user@host# edit chassis fpc 0 pic 0
[edit chassis fpc - pic 0]

```
2. Set the bandwidth for inline services.  

```

[edit chassis fpc 0 pic 0]

```

```
user@host# set inline-services bandwidth 10g
```

### Configuring NAT Pool and Rule

#### Step-by-Step Procedure

1. Go to the services NAT hierarchy.  

```
user@host# edit services nat
```
2. Configure three NAT pools.  

```
[edit services nat]
user@host# set nat pool p1 address 20.1.1.0/24
user@host# set nat pool p2 address 21.1.1.2/32
user@host# set nat pool p3 address 120.1.1.1/32
```
3. Configure NAT rule for source pool p1.  

```
[edit services nat]
user@host# set nat rule r1 match-direction input
user@host# set nat rule r1 term t1 from source-address 10.1.1.0/24 then
[nat pool r1 term t1 from source-address 10.1.1.0/24 then]
user@host# set translated source-pool p1 translation-type basic-nat44
```
4. Configure NAT rule for source pool p2.  

```
[edit services nat]
user@host# set nat rule r2 match-direction input
user@host# edit nat rule r2 term t1 from source-address 192.168.1.2/32 then
[nat pool r2 term t1 from source-address 192.168.1.2/32 then]
user@host# set translated source-pool p2 translation-type basic-nat44.
```
5. Configure NAT rule for source pool p3.  

```
[edit services nat]
user@host# set nat rule r3 match-direction input
user@host# edit nat rule r3 term t1 from source-address 10.1.1.8/32 then
[nat pool r1 term t1 from source-address 10.1.1.8/32 then]
user@host# set translated source-pool p1 translation-type basic-nat44
```

```
Results user@host# edit services nat
user@host# show

pool p1 {
    address 20.1.1.0/24;
}
pool p2 {
    address 21.1.1.2/32;
}
pool p3 {
    address 120.1.1.1/32;
}
rule r1 {
    match-direction input;
    term t1 {
        from {
            source-address {
                10.1.1.0/24;
            }
        }
        then {
            translated {
                source-pool p1;
                translation-type {
                    basic-nat44;
                }
            }
        }
    }
}
rule r2 {
    match-direction input;
    term t1 {
        from {
            source-address {
                192.168.1.2/32;
            }
        }
        then {
            translated {
                source-pool p2;
                translation-type {
                    basic-nat44;
                }
            }
        }
    }
}
rule r3 {
    match-direction input;
    term t1 {
        from {
            source-address {
                10.1.1.8/32;
            }
        }
        then {
            translated {
                source-pool p3;
                translation-type {
```

```

        basic-nat44;
    }
}
}
}
}

```

### Configuring the Service Set

#### Step-by-Step Procedure

1. Configure a service set using NAT rule r1, associated with NAT pool p1.  

```

user@host# edit services service-set nat1
[edit services service-set nat1]
user@host# set nat rules r1
user@host# set interface-service service-interface si-0/0/0.0

```
2. Configure a service set using NAT rule r2, associated with NAT pool p2.  

```

user@host# edit services service-set nat2
[edit services service-set nat1]
user@host# set nat rules r2
user@host# set interface-service service-interface si-0/0/0.0

```
3. Configure a service set using NAT rule r3, associated with NAT pool p3.  

```

user@host# edit services service-set nat3
[edit services service-set nat1]
user@host# set nat rules r3
user@host# set interface-service service-interface si-0/0/0.0

```

#### Results

```

user@host# edit services service-set nat1
user@host# show
nat-rules r1;
interface-service {
    service-interface si-0/0/0.0;
}

user@host# edit services service-set nat2
user@host# show
nat-rules r2;
interface-service {
    service-interface si-0/0/0.0;
}

user@host# edit services service-set nat3
user@host# show
nat-rules r3;
interface-service {
    service-interface si-0/0/0.0;
}

```

#### Related Documentation

- [Inline Network Address Translation Overview for MPC Types 1, 2, and 3 on page 59](#)

## Port Control Protocol Configuration Examples

This topic contains the following Port Control Protocol (PCP) configuration examples.

- [Example: Configuring Port Control Protocol with NAPT44 on page 290](#)

### Example: Configuring Port Control Protocol with NAPT44

- [Requirements on page 290](#)
- [Overview on page 290](#)
- [PCP Configuration on page 290](#)

#### Requirements

Hardware Requirements

- UEs with PCP clients.
- An MX 3D Router with an MS-DPC services PIC.

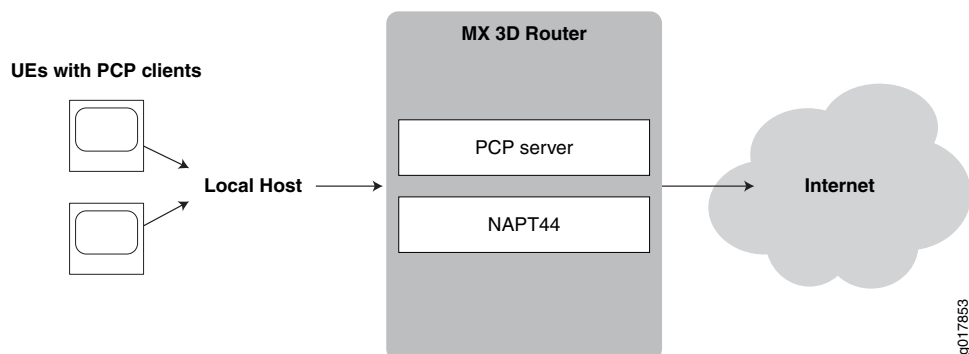
Software Requirements

- Junos OS 13.2
- Layer-3 Services Package

#### Overview

An ISP wants to enable UEs with PCP clients to maintain connections to servers without timing out. The PCP clients generate PCP requests for the type and duration of the connection they require. Connections may be of a long duration, such as applications using a webcam, or a shorter duration, such as online games. An MX 3D router provides a PCP server to interpret PCP client requests, and NAPT44. [Figure 15 on page 290](#) shows the basic topology for this example.

Figure 15: PCP with NAPT44



#### PCP Configuration

##### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network

configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```

set chassis fpc 2 pic 0 adaptive-services service-package layer-3
set interfaces sp-2/0/0 services-options inactivity-timeout 180 cgn-pic
set interfaces sp-2/0/0 unit 0 family inet
set interfaces xe-3/2/0 unit 0 family inet service input service-set sset_0
set interfaces xe-3/2/0 unit 0 family inet service output service-set sset_0
set interfaces xe-3/2/0 unit 0 family inet address 30.0.0.1/24
set interfaces xe-5/0/0 unit 0 family inet address 25.0.0.1/24
set services nat pool pcp-pool address 44.0.0.0/16
set services nat pool pcp-pool port automatic random-allocation address-allocation
    round-robin
set services nat pool pcp-pool address-allocation round-robin
set services nat rule pcp-rule match-direction input
set services nat rule pcp-rule term t0 then translated source-pool pcp-pool
    translation-type napt-44
set services nat rule pcp-rule term t0 then translated mapping-type endpoint-independent
    filtering-type endpoint-independent
set services nat rule pcp-rule term t0 then translated mapping-type endpoint-independent
    filtering-type endpoint-independent
set services pcp server pcp-s1 ipv4-address 124.124.124.122 mapping-lifetime-minimum
    600 mapping-lifetime-minimum 600
set services pcp server pcp-s1 mapping-lifetime-minimum 600
    mapping-lifetime-maximum 86500
set services pcp server pcp-s1 short-lifetime-error 120 long-lifetime-error 1200
set services pcp server pcp-s1 max-mappings-per-client 128 pcp-options third-party
    prefer-failure
set services service-set sset_0 pcp-rules r1
set services service-set sset_0 nat-rules pcp-rule
set services service-set sset_0 interface-service service-interface sp-2/0/0.0

```

### *Chassis Configuration*

**Step-by-Step Procedure** To configure the service PIC (FPC 2 Slot 0) with the Layer 3 service package:

1. Go to the [edit chassis] hierarchy level.  

```
user@host# edit chassis
```
2. Configure the Layer 3 service package.  

```
[edit chassis]
user@host# set fpc 2 pic 0 adaptive-services service-package layer-3
```

**Results**    user@host# show chassis fpc 2 pic 0

```
pcp-rules pcp-napt44-rule;
nat-rules pcp-rule;
interface-service {
    service-interface sp-2/0/0.0;
}
```

### *Interface Configuration*

**Step-by-Step  
Procedure**

1.    Configure the services MS-DPC.  

```
user@host# set interfaces sp-2/0/0 services-options inactivity-timeout 180 cgn-pic
user@host# set interfaces sp-2/0/0 unit 0 family inet
```
2.    Configure the customer-facing interface used for NAT and PCP services.  

```
user@host# set interfaces xe-3/2/0 unit 0 family inet service input service-set
sset_0
user@host# set interfaces xe-3/2/0 unit 0 family inet service output service-set
sset_0
user@host# set interfaces xe-3/2/0 unit 0 family inet address 30.0.0.1/24
```
3.    Configure the Internet-facing interface.  

```
user@host# set interfaces xe-5/0/0 unit 0 family inet address 25.0.0.1/24
```

**Results**

```

user@host#
sp-2/0/0 {
  services-options {
    inactivity-timeout 180;
    cgn-pic;
  }
  unit 0 {
    family inet;
  }
}
xe-3/2/0 {
  unit 0 {
    family inet {
      service {
        input {
          service-set sset_0;
        }
        output {
          service-set sset_0;
        }
      }
      address 30.0.0.1/24;
    }
  }
}
xe-5/0/0 {
  unit 0 {
    family inet {
      address 25.0.0.1/24;
    }
  }
}

```

### *NAT Configuration*

#### **Step-by-Step Procedure**

1. Go the [edit services nat] hierarchy.  

```

user@host# edit services nat

```
2. Configure a NAT pool called **pcp-pool**.  

```

[edit services nat]
user@host# set pool pcp-pool address 44.0.0.0/16
user@host# set pool pcp-pool port automatic random-allocation
user@host# set pool pcp-pool address-allocation round-robin

```
3. Configure a NAT rule called **pcp-rule**.  

```

[edit services nat]
user@host# set rule pcp-rule term t0 then translated source-pool pcp-pool
translation-type napt-44
user@host# set rule pcp-rule term t0 then translated mapping-type
endpoint-independent filtering-type endpoint-independent

```

```

Results user@host# show services nat
pool pcp-pool {
    address 44.0.0.0/16;
    port {
        automatic {
            random-allocation;
        }
    }
    address-allocation round-robin;
}
rule pcp-rule {
    match-direction input;
    term t0 {
        then {
            translated {
                source-pool pcp-pool;
                translation-type {
                    napt-44;
                }
                mapping-type endpoint-independent;
                filtering-type {
                    endpoint-independent;
                }
            }
        }
    }
}

```

### PCP Configuration

**Step-by-Step Procedure** To configure the PCP server and PCP rule options.

1. Go to the **edit services pcp** hierarchy level for server **pcp-s1**  

```
user@host# edit services pcp server pcp-s1
```
2. Configure the PCP server options.  

```
[edit services pcp server pcp-s1]
user@host# set ipv4-address 124.124.124.122
user@host# set mapping-lifetime-minimum 600
user@host# set mapping-lifetime-maximum 86500
user@host# set short-lifetime-error 120
user@host# set long-lifetime-error 1200
user@host# set max-mappings-per-client 128
user@host# set pcp-options third-party prefer-failure
```
3. Create the PCP rule.  

```
[edit services pcp rule pcp-napt44-rule]
user@host# edit rule pcp-napt44-rule
```
4. Configure the PCP rule options.  

```
[edit services pcp rule pcp-napt44-rule]
user@host# set match-direction input
user@host# set term t0 then pcp-server pcp-s1
```

**Results** regress@montag# show services pcp

```
server pcp-s1 {
    ipv4-address 124.124.124.122;
    mapping-lifetime-minimum 600;
    mapping-lifetime-maximum 86500;
    short-lifetime-error 120;
    long-lifetime-error 1200;
    max-mappings-per-client 128;
    pcp-options third-party prefer-failure;
}
rule pcp-napt44-rule {
    match-direction input;
    term t0 {
        then {
            pcp-server pcp-s1;
        }
    }
}
```

### Service Set Configuration

- Step-by-Step Procedure**
1. Create a service set, **sset\_0**, at the **edit services service-set** hierarchy level.

```
user@router# edit services service-set sset_0

service-set sset_0 {
    pcp-rules pcp-napt44-rule;
    nat-rules pcp-rule;
    interface-service {
        service-interface sp-2/0/0.0;
    }
}
```

2. Identify the NAT rule associated with the service set.
 

```
[edit services service-set sset_0]
user@router# set nat-rules pcp-rule
```
3. Identify the PCP rule associated with the service set.
 

```
[edit services service-set sset_0]
user@router# set pcp-rules r1
```
4. Identify the service interface associated with the service set.
 

```
[edit services service-set sset_0]
user@router# set interface-service service-interface sp-2/0/0.0
```

**Results**    user@host# show  
pcp-rules pcp-napt44-rule;  
nat-rules pcp-rule;  
interface-service {  
    service-interface sp-2/0/0.0;  
}

---

## Carrier-Grade NAT Implementation: Best Practices

The following topics present the best practices for carrier-grade NAT implementation on MS-DPCs using the Layer 3 services package:

- [Use APP and Round-Robin Address-Allocation on page 296](#)
- [Do Not Use EIM with SIP on page 297](#)
- [Do Not Use EIM with HTTP, DNS, or When Not Needed on page 297](#)
- [Define PBA Blocks Based on User Profiles on page 298](#)
- [Do Not Change the PBA Configuration on Running Systems on page 299](#)
- [Do Not Allocate Excessively Large NAT Pools on page 300](#)
- [Configure the System Log for PBA Only When Needed on page 300](#)
- [Use Redundant Service PIC \(RSP\) Interfaces for Failover on page 302](#)
- [Contain the Effects of Missing IP Fragments on page 303](#)
- [Do Not Use Configurations Prone to Routing Loops on page 303](#)

### Use APP and Round-Robin Address-Allocation

#### Scenario:

- Address-pooling paired (APP) allows a private IP address to be mapped to the same public IP address from a NAT pool for all its sessions. The binding between private IP and public IP is triggered by the first packet seen from such private host.
- By default, an MS-DPC or MS-PIC allocates ports from a NAT pool in a sequential fashion from each consecutive IP address available in the pool.
- Sequential allocation, together with APP, can result in mapping multiple private hosts to the same public IP address, resulting in fast port exhaustion for the interested public IP address while other ports are still available from the remaining of NAT pool.



**BEST PRACTICE:** Configure round-robin address allocation for the NAT pool used by traffic served with APP. Round-robin allocation allocates ports from different IP addresses.

---

The following snippet provides an example of round-robin address allocation.

```
user@router# show services nat pool natpool-1
address-range low 9.9.9.1 high 9.9.9.10;
port {
    automatic;
```

```

}
address-allocation round-robin;
mapping-timeout 120;

```

**Related Documentation**

- *Round-Robin Allocation in (OBSOLETE) Network Address Translation Configuration Components Overview.*

## Do Not Use EIM with SIP

### Scenario:

- Session Initiation Protocol (SIP) traffic requires an Application Level Gateway (ALG) to allow SIP servers and clients on the public side of the CGNAT to communicate with the SIP hosts on the private side.
- The SIP ALG opens the pinholes in the CGNAT router to permit the forwarding of outbound traffic based on any supported SIP feature.
- Endpoint-independent mapping (EIM) is not needed by SIP to function, nor by the SIP ALG to create the flows for forwarding the SIP traffic



**BEST PRACTICE:** Do *not* configure EIM together with the SIP ALG; doing so adds processing overhead with no benefit.

```

user@router# show services nat rule natrule-1
match-direction input;
term 1 {
  from {
    applications junos-sip;
  }
  then {
    translated {
      source-pool natpool-3;
      translation-type {
        napt-44;
      }
      address-pooling paired;
    }
  }
}

```

## Do Not Use EIM with HTTP, DNS, or When Not Needed

### Scenario:

- Most Internet traffic uses HTTP, and there is no browser on any OS that reuses the same source port for sending traffic to different destinations. EIM provides no benefit for HTTP traffic.
- Because none of the junos-algs require EIM to work, avoid using EIM with the ALGs.
- EIM allocates memory for each mapping; this is in addition to the memory used for flow allocation. This reduces the maximum number of flows that can be established through the services PIC, and causes processing overhead for the creation and deletion of flows and mappings.

**BEST PRACTICE:**

- Don't enable EIM for applications that are defined ALGs or are known not to use Session Traversal Utilities for NAT (STUN) servers to discover the presence of a NAT router.
- Enable EIM for applications that do reuse the source ports and rely on a CGNAT device to maintain the same address:port mapping for all traffic sent to different destinations, such as on-line gaming applications like Xbox and PS3, or applications that use unilateral self-address fixing methods (UNSAF). see (*IETF RFC 3424 IAB Considerations for UNilateral Self-Address Fixing (UNSAF) Across Network Address Translation*).

## Define PBA Blocks Based on User Profiles

**Scenario:**

- When a user connects to a website that requires the establishment of a significant number of sockets for a single HTML page, a corresponding number of new ports must be allocated. Port blocks should be large enough to prevent continual allocation of new blocks.
- If the number of concurrent sessions exceeds the number of ports available in the active port block, the other allocated port-blocks will be scanned for available ports to use or a new block will be allocated from the free block pool.
- The process of continually scanning the allocated port-blocks and/or allocating additional blocks from the free block pool could result in experienced latency for setting up new sessions and delay loading of web pages.
- Having a user continuously allocating or de-allocating from different PBA blocks impacts performance.



**BEST PRACTICE:** Define PBA blocks with a size that is a power of 2 or 4 related to the average number of sessions a user is expected to have active. For example, if a user is expected to have an average of approximately 200 to 250 sessions active, configuring the PBA block size to 512 or 1024 will provide a liberal allocation.

```
user@router# show services nat pool natpool-1
address-range low 9.9.9.1 high 9.9.9.10;
  port {
    automatic;
    secure-port-block-allocation {
      block-size 1024;
      max-blocks-per-user 8; /* Max 2048, default 8 */
      active-block-timeout 300;
    }
  }
mapping-timeout 300;
```

- Related Documentation**
- *Port Block Allocation in (OBSOLETE) Network Address Translation Configuration Components Overview.*

## Do Not Change the PBA Configuration on Running Systems

### Scenario:

- PBA settings in NAT pools are mapped to memory at the time of the Service PIC boot up and cannot be changed while processing traffic.
- Do not change the following settings:
  - Update any NAT pool PBA configuration.
  - Change a PBA NAT pool to a non-PBA NAT pool.
  - Change a non-PBA NAT pool to a PBA NAT pool.

Any of these changes result in the logging of the following message:

PBA\_CATASTROPIC\_CHANGE: The recent PBA configuration changes will reflect in the Service-PIC only after deactivate and activate of the service-set again



**NOTE:** Starting with Junos OS Release 14.1, when you deactivate a service-set that contains address pooling paired (APP) or endpoint independent mapping (EIM) mapping for that service-set, messages are displayed on the PIC console and the mappings are cleared for that service-set. These messages are triggered when the deletion of a service-set commences and again generated when the deletion of the service-set is completed. The following sample messages are displayed when deletion starts and ends:

- Nov 15 08:33:13.974 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion initiated
- Nov 15 08:33:14.674 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion completed

In a scaled environment that contains a large number of APP or EIM mappings in a service set, a heavy volume of messages is generated and this process takes some amount of time. We recommend that you wait until the console messages indicating the completion of deletion of the service set are completed before you reactivate the service-set again.



**BEST PRACTICE:** When changing PBA configurations, restart the services PIC if possible. Minimally, you must deactivate and reactivate the affected service set.

- Related Documentation**
- *Port Block Allocation in (OBSOLETE) Network Address Translation Configuration Components Overview.*

## Do Not Allocate Excessively Large NAT Pools

### Scenario:

- The maximum number of flows supported by the MS-DPC and each PIC on an MS-DPC is 8 million.
- Assuming that the 8 million flow maximum consists of 4 million sessions (1 reverse flow for each forward flow), these sessions would require a maximum of 4 million ports that are available from 64 IP addresses within the 1024 to 65,535 ports range (64K ports per IP address).
- Do not configure ports to support more than 8 million flows; they will never be needed.
- This scenario assumes that APP, EIM, and EIF are not enabled. When they *are* enabled, the total number of flows is lower, which means that you should configure the number of IP addresses in the NAT pool based on the maximum supported flows.



**BEST PRACTICE:** Do not configure NAT pools with more than 64 addresses (that is, a /26 network) and round-robin configured and 64K ports from each address.

---

## Configure the System Log for PBA Only When Needed

### Scenario:

- Session logging can negatively affect performance depending on the frequency of creation and deletion of flows.
- PBA is meant to reduce the need for logging.
- Deterministic NAT is designed to eliminate the need for logging.
- All system log messages created by the services PIC constitutes traffic that will be sent to the Packet Forwarding Engine, competing with user traffic to reach the external destination.



### BEST PRACTICE:

- Use logging to the system log at the service-set level rather than at the services PIC interface level when possible.
- Do not enable logging for redundant information. When using PBA, you don't need to configure logs per session because knowing the PBA block and the block size enables you to derive the ports allocated to each user. In this case, a log that reports all sessions created by that user with ports belonging to a block is redundant. If you have configured deterministic NAT

(DetNat) a log is completely unnecessary because all information on port allocation can be deduced mathematically.

- Rate-limit the number of logs generated from an sp- interface. When not set, the default limits apply: 10K for the local host system log server (RE) and 200K for the external system log server.

```
user@router# show interfaces sp-1/1/0 services-options
system log {
  host 1.2.3.4 {
    services info;
  }
  message-rate-limit 1000;
}
```

- Always system log to an external server to avoid loading the Routing Engine and specify system log class to restrict logging.
  - If you do not specify system log class, all log messages are allowed (subject to priority check and rate limiting).
  - When you specify system log class, only messages meeting the class criteria are retained.
  - Use the `show services service-sets statistics system log detail` command to check what is being dropped by unconfigured classes.

```
user@router# show services service-set S-SET-1 system log
host 1.2.3.4 {
  services info;
  class {
    session-logs open close;
    packet-logs;
    stateful-firewall-logs;
    alg-logs;
    nat-logs;
    ids-logs;
  }
}
```



**BEST PRACTICE:** System log generation can be *rule-based* or *event-based*.

- Use rule-based system logging with care; it generates a log for every packet that enters the rule term, since rule-based logging is not subject to class or priority filtering.
- System log messages can be dropped only as a result of message rate limiting. Make sure you have set a realistic rate-limit that is unlikely to be exceeded.
- Use rule-based logging only for discarded traffic (a relatively small percentage of the traffic) or for troubleshooting. Since rule-based logging applies to all traffic that enters the PIC and creates a flow, logging can be excessive, resulting in reaching the configured induce rate limit with a consequent loss of needed logs.

```
cli# show services stateful-firewall
```

```
rule rule-sfw-accept {
    match-direction input-output;
    term term-sfw-accept {
        then {
            accept;
            system log;
        }
    }
}
rule rule-sfw-reject {
    match-direction input-output;
    term term-sfw-reject {
        then {
            reject;
            system log;
        }
    }
}
```



---

**BEST PRACTICE:**

All rule match logs are enabled by their respective rules:

- ASP\_COS\_RULE\_MATCH (class-of-service rules)
  - ASP\_COS\_RULE\_MATCH (class-of-service rules)
  - ASP\_IDS\_RULE\_MATCH (ids rules)
  - ASP\_NAT\_RULE\_MATCH (nat rule)
  - ASP\_SFW\_RULE\_ACCEPT (stateful firewall rules)
  - ASP\_SFW\_RULE\_DISCARD
  - ASP\_SFW\_RULE\_REJECT
- 

## Use Redundant Service PIC (RSP) Interfaces for Failover

---

**BEST PRACTICE:**

- The usage of Redundant Service PIC (RSP) interfaces, allows the active services PIC to perform an immediated switchover to the secondary services PIC in case of major issues that require a services PIC reboot.
- This results in a minimal service impact for user traffic.
- There are two modes for redunancy: warm-standby (default) and hot-standby. Hot-standby provides 1:1 redundancy, while warm-standby provides 1:N redundancy. With both modes , there is no impact on the UDP forwarding.

- When the secondary services PIC is shared among multiple RSPs, only warm-standby is possible and the impact to traffic is limited to the time to load the appropriate configuration on the secondary PIC.

```
user@router# show interfaces rsp0
redundancy-options {
    primary sp-0/1/0;
    secondary sp-1/1/0;
    hot-standby;
}
```

## Contain the Effects of Missing IP Fragments

### Scenario:

- IP fragments are buffered as they arrive to facilitate the integrity check of the completely reassembled packet before being serviced by the services PIC.
- Missing fragments cause received fragments to be held until the internal buffer is full and are flushed out. This causes CPU usage overhead and reduced traffic forwarding.



**BEST PRACTICE:** Configure the **fragment-limit**, the maximum number of fragments for a packet, and **reassembly-timeout**, the maximum wait for a missing fragment, after which all other fragments for the same packet are flushed out.

```
user@router# show interfaces sp-0/0/0
services-options {
    open-timeout 5;
    close-timeout 5;
    inactivity-timeout 30;
    tcp-tickles 4;
    fragment-limit 10;
    reassembly-timeout 3;
    cgn-pic;
}
```

## Do Not Use Configurations Prone to Routing Loops

### Scenario:

- Sudden and persistent high CPU usage is most likely an indication of packet looping between the Packet Forwarding Engine and the services PIC. Depending on whether the configuration uses interface-style or next-hop-style service sets, different network flaps can lead to routing loops.



**BEST PRACTICE:**

Ensure that only the intended traffic is allowed to reach the services PIC and is serviced based on service set rule.

- Configure a firewall filter that accepts only the traffic meant to go to the services PIC on the output direction of the sp- interface. That is, accept only traffic identified in the NAT rule from option as received from the source-address that identifies the customer private network; discard and log all the rest.
  - Allow only intended traffic to be serviced by the service set by configuring the stateful-firewall rules and NAT rules to translate only the traffic from the customer private source address ranges and intended applications. Although this does not prevent unintended traffic from being processed by the services PIC, it prevents the creation of flows, objects, and states that are not consistent with the expected traffic and are likely to be problematic.
-

## CHAPTER 7

# Summary of Network Address Translation Configuration Statements

The following sections explain each of the network address translation services statements. The statements are organized alphabetically.

- [address \(Services NAT Pool\) on page 307](#)
- [address-allocation on page 307](#)
- [address-range on page 308](#)
- [allow-overlapping-nat-pools on page 308](#)
- [app-mapping-timeout on page 309](#)
- [application-sets \(Services NAT\) on page 309](#)
- [applications \(Services NAT\) on page 310](#)
- [cgn-pic on page 310](#)
- [destination-address on page 311](#)
- [destination-address-range on page 312](#)
- [destination-pool on page 312](#)
- [destination-port range on page 313](#)
- [destination-prefix on page 313](#)
- [destination-prefix-list on page 314](#)
- [destined-port on page 314](#)
- [deterministic-port-block-allocation on page 315](#)
- [dns-alg-pool on page 316](#)
- [dns-alg-prefix on page 316](#)
- [ei-mapping-timeout on page 317](#)
- [eif-flow-limit on page 317](#)
- [from \(Services NAT\) on page 318](#)
- [ipv6-multicast-interfaces on page 319](#)
- [mapping-refresh on page 319](#)
- [mapping-timeout on page 320](#)

- [match-direction on page 320](#)
- [no-translation on page 321](#)
- [overload-pool on page 321](#)
- [overload-prefix on page 322](#)
- [pool on page 323](#)
- [port on page 324](#)
- [port-forwarding on page 325](#)
- [port-forwarding-mappings on page 325](#)
- [ports-per-session on page 326](#)
- [rule on page 327](#)
- [rule-set on page 328](#)
- [secure-nat-mapping on page 328](#)
- [secured-port-block-allocation on page 329](#)
- [server \(pcp\) on page 330](#)
- [services \(NAT\) on page 331](#)
- [service-set \(Services\) on page 332](#)
- [source-address \(NAT\) on page 334](#)
- [source-address-range on page 334](#)
- [source-pool on page 335](#)
- [source-prefix on page 335](#)
- [source-prefix-list on page 336](#)
- [syslog on page 336](#)
- [translated-port on page 337](#)
- [term on page 338](#)
- [then on page 339](#)
- [translated on page 340](#)
- [translation-type on page 341](#)

## address (Services NAT Pool)

---

<b>Syntax</b>	<code>address ip-prefix&lt;/prefix-length&gt;;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> nat-pool-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <i>prefix</i> option enhanced to support IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Specify the NAT pool prefix value.
<b>Options</b>	<i>prefix</i> —Specify an IPv4 or IPv6 prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Source and Destination Addresses Network Address Translation Overview on page 191</a></li></ul>

## address-allocation

---

<b>Syntax</b>	<code>address-allocation round-robin;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> pool-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	When you use round-robin allocation, one port is allocated from each address in a range before repeating the process for each address in the next range. After ports have been allocated for all addresses in the last range, the allocation process wraps around and allocates the next unused port for addresses in the first range.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Pools of Addresses and Ports for Network Address Translation Overview on page 192</a></li></ul>

## address-range

---

<b>Syntax</b>	address-range low <i>minimum-value</i> high <i>maximum-value</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> nat-pool-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <i>minimum-value</i> and <i>maximum-value</i> options enhanced to support IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Specify the NAT pool address range.
<b>Options</b>	<i>minimum-value</i> —Lower boundary for the IPv4 or IPv6 address range. <i>maximum-value</i> —Upper boundary for the IPv4 or IPv6 address range.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Source and Destination Addresses Network Address Translation Overview on page 191</a></li></ul>

## allow-overlapping-nat-pools

---

<b>Syntax</b>	allow-overlapping-nat-pools;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat]
<b>Release Information</b>	Statement introduced with Junos OS Release 12.1.
<b>Description</b>	Specify that NAT source or destination pools can be shared between multiple service sets.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Sets for Network Address Translation on page 209</a></li></ul>

## app-mapping-timeout

---

<b>Syntax</b>	<code>app-mapping-timeout <i>app-mapping-timeout</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> <i>nat-pool-name</i> ]
<b>Release Information</b>	<code>mapping-timeout</code> statement introduced in JUNOS Release 12.3.
<b>Description</b>	Specify the duration for address pooling paired (AP-P) mappings that use the specified NAT pool. If this option is not configured and a timeout value is configured for <a href="#">mapping-timeout</a> , the timeout value configured for <a href="#">mapping-timeout</a> is used. If neither option is specified, the default value of 300 seconds is used.
<b>Options</b>	<p><code>app-mapping-timeout</code>—Lifetime of AP-P mappings in seconds.</p> <p><b>Default:</b> 300</p> <p><b>Range:</b> 120 through 864,000</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Source and Destination Addresses Network Address Translation Overview on page 191</a></li> </ul>

## application-sets (Services NAT)

---

<b>Syntax</b>	<code>applications-sets <i>set-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define one or more target application sets.
<b>Options</b>	<code>set-name</code> —Name of the target application set.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li> </ul>

## applications (Services NAT)

---

<b>Syntax</b>	<code>applications [ <i>application-names</i> ];</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define one or more application protocols to which the NAT services apply.
<b>Options</b>	<i>application-name</i> —Name of the target application.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## cgn-pic

---

<b>Syntax</b>	<code>cgn-pic;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Restrict usage of the service PIC to carrier-grade NAT (CGN) or associated services (intrusion detection, stateful firewall, and software). All memory is available for CGN or related services and can be used for CGN scaling.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card on page 60</a></li></ul>

## destination-address

---

<b>Syntax</b>	<code>destination-address (<i>address</i>   any-unicast) &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>any-unicast</b> and <b>except</b> options introduced in Junos OS Release 7.6. <b>address</b> option enhanced to support IPv6 and addresses in Junos OS Release 8.5.
<b>Description</b>	Specify the destination address for rule matching.
<b>Options</b>	<b>address</b> —Destination IPv4 or IPv6 address or prefix value.  <b>any-unicast</b> —Any unicast packet.  <b>except</b> —(Optional) Prevent the specified address, prefix, or unicast packets from being translated.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## destination-address-range

---

Syntax	destination-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>;
Hierarchy Level	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
Release Information	Statement introduced in Junos OS Release 7.6. <i>minimum-value</i> and <i>maximum-value</i> options enhanced to support IPv6 addresses in Junos OS Release 8.5.
Description	Specify the destination address range for rule matching.  If the <a href="#">translation-type</a> statement in the <a href="#">then</a> statement of the nat rule is set to <b>stateful-nat-64</b> , the destination address range for rule matching must be within the range specified by the <a href="#">destination-prefix</a> statement in the <a href="#">then</a> statement.
Options	<i>minimum-value</i> —Lower boundary for the IPv4 or IPv6 address range.  <i>maximum-value</i> —Upper boundary for the IPv4 or IPv6 address range.  <i>except</i> —(Optional) Prevent the specified address range from being translated.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## destination-pool

---

Syntax	destination-pool <i>nat-pool-name</i> ;
Hierarchy Level	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then translated</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the destination address pool for translated traffic.
Options	<i>nat-pool-name</i> —Destination pool name.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## destination-port range

---

<b>Syntax</b>	<code>destination-port range <i>high</i>   <i>low</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> (Services NAT)]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Specify the destination port range for rule matching.
<b>Options</b>	<i>high</i> —Upper limit of port range for matching. <i>low</i> —Lower limit of port range for matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port Forwarding for Static Destination Address Translation on page 251</a></li></ul>

## destination-prefix

---

<b>Syntax</b>	<code>destination-prefix <i>destination-prefix</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then translated</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6. <i>destination-prefix</i> option enhanced to support IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Specify the destination prefix for translated traffic.
<b>Options</b>	<i>destination-prefix</i> —IPv4 or IPv6 destination prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## destination-prefix-list

---


<b>Syntax</b>	<code>destination-prefix-list <i>list-name</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	<p>Specify the destination prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the <b>[edit policy-options]</b> hierarchy level.</p> <p>If the <a href="#">translation-type</a> statement in the <a href="#">then</a> statement of the nat rule is set to <b>stateful-nat-64</b>, the destination prefix list for rule matching must be within the range specified by the <a href="#">destination-prefix</a> statement in the <a href="#">then</a> statement.</p>
<b>Options</b>	<p><i>list-name</i>—Destination prefix list.</p> <p><b>except</b>—(Optional) Exclude the specified prefix list from rule matching.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li><li>• <a href="#">Routing Policy Feature Guide for Routing Devices</a></li></ul>

## destined-port

---

<b>Syntax</b>	<code>destined-port <i>port id</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">port-forwarding</a> <i>map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Specify the port from where traffic has to be forwarded.
<b>Options</b>	<p><i>port id</i>—The destination port number from where traffic will be forwarded.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">port-forwarding on page 325</a></li><li>• <a href="#">translated-port on page 337</a></li></ul>

## deterministic-port-block-allocation

<b>Syntax</b>	deterministic-port-block-allocation { block-size <i>block-size</i> ; include-boundary-addresses; }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> <i>pool-name</i> port]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Configure algorithm-based allocation of blocks of destination ports. By specifying this method, you ensure that an incoming (source) IP address and port always map to the same destination IP address and port block, thus eliminating the need for logging address translations.
<b>Options</b>	<b>block-size</b> —Maximum number of ports that can be allocated to a user.
<div>  <p><b>NOTE:</b> When a <b>block-size</b> of 0 is specified, block size is calculated according to the formula: <math>(64512 * \text{Number of IP addresses in the NAT Pool}) / \text{Number of subscribers}</math> where</p> <ul style="list-style-type: none"> <li>64512 is derived from <math>(65535 - 1023)</math> because the regular port assignments start from 1024.</li> <li>Number of subscribers is derived from the <b>from</b> clause of the applicable NAT rule.</li> </ul> </div>	
<p><b>Default:</b> 256</p> <p><b>Range:</b> 0 through 32,000</p> <p><b>include-boundary-addresses</b>—(Optional) Specifies that the lowest and highest addresses in the source address range of a NAT rule should be translated when the NAT pool is used.</p>	
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring Deterministic Port Block Allocation on page 237</a></li> </ul>

## dns-alg-pool

---

<b>Syntax</b>	<code>dns-alg-pool <i>dns-alg-pool</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then translated</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the Network Address Translation (NAT) pool for destination translation.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## dns-alg-prefix

---

<b>Syntax</b>	<code>dns-alg-prefix <i>dns-alg-prefix</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then translated</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Set the Domain Name System (DNS) application-level gateway (ALG) 96-bit prefix for mapping IPv4 addresses to IPv6 addresses.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## ei-mapping-timeout

<b>Syntax</b>	mapping-timeout <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> <i>nat-pool-name</i> ]
<b>Release Information</b>	ei-mapping-timeout statement introduced in JUNOS Releases 12.3.
<b>Description</b>	Specify the duration for endpoint independent translations that use the specified NAT pool. This includes endpoint-independent mapping (EIM) and endpoint-independent filtering (EIF).
<b>Options</b>	<i>seconds</i> —Lifetime of endpoint independent mappings in seconds. <b>Default:</b> 300 <b>Range:</b> 120 through 864,000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Network Address Translation Configuration Overview on page 191</a></li> </ul>

## eif-flow-limit

<b>Syntax</b>	eif-flow-limit <i>number-of-flows</i>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then translated secure-nat-mapping</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3
<b>Description</b>	Specify the maximum number of inbound flows allowed on EIF mapping to the configured value. This limit is per EIF mapping and is per given instance of time. For example, if <b>eif-flow-limit</b> is configured as n, then only n inbound connections are allowed at a given instance of time. The n+1 and subsequent connections arriving when n connections are alive are dropped. A new inbound connection is allowed only when one of the n connections times out or is closed. This limit is applied for all type of flows.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## from (Services NAT)

---

<b>Syntax</b>	<pre>from {   application-sets set-name;   applications [ application-names ];   destination-address (address   any-unicast) &lt;except&gt;;   destination-address-range low minimum-value high maximum-value &lt;except&gt;;   source-address address (address   any-unicast) &lt;except&gt;;   source-address-range low minimum-value high maximum-value &lt;except&gt;; }</pre>
<b>Hierarchy Level</b>	[edit <b>services</b> nat <b>rule</b> rule-name <b>term</b> term-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify input conditions for the NAT term.
<b>Options</b>	<p>For information on match conditions, see the description of firewall filter match conditions in the <i>Routing Policy Feature Guide for Routing Devices</i>.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## ipv6-multicast-interfaces

<b>Syntax</b>	ipv6-multicast-interfaces (all   <i>interface-name</i> ) { disable; }
<b>Hierarchy Level</b>	[edit <a href="#">services nat</a> ], [edit services software]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Enable multicast filters on Ethernet interfaces when IPv6 NAT is used for neighbor discovery.
<b>Options</b>	<p><b>all</b>—Enable filters on all interfaces.</p> <p><b>disable</b>—Disable filters on the specified interfaces.</p> <p><b><i>interface-name</i></b>—Enable filters on a specific interface only.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring IPv6 Multicast Interfaces</i></li> </ul>

## mapping-refresh

<b>Syntax</b>	mapping-refresh nbound   outbound   inbound-outbound);
<b>Hierarchy Level</b>	[edit <a href="#">services nat rule rule-name term term-name then translated secure-nat-mapping</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3
<b>Description</b>	Specify how the flow timer should be refreshed based on the mapping refresh configured for all types of fwnat flows. For TCP flows, if <b>tcp-tickles</b> is configured, then tickles are sent only on the flow matching the mapping-refresh direction. For inbound-outbound mapping, refresh tickles will be sent on both the flows (default behavior).
<b>Options</b>	<p><b>inbound</b>—Refresh the flow timer for inbound flows only.</p> <p><b>inbound-outbound</b>—Refresh the flow timer for all flows.</p> <p><b>outbound</b>—Refresh the flow timer for outbound flows only.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>•</li> </ul>

## mapping-timeout

---

<b>Syntax</b>	mapping-timeout <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> <i>nat-pool-name</i> ]
<b>Release Information</b>	mapping-timeout statement introduced in JUNOS Release 10.1.



**NOTE:** This configuration option has been replaced by [app-mapping-timeout](#). This option is currently retained only for backward compatibility.

---

<b>Description</b>	Specify the duration for mappings that use the specified NAT pool.
<b>Options</b>	<b>seconds</b> —Lifetime of mappings in seconds. <b>Default:</b> 300 <b>Range:</b> 120 through 864,000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Source and Destination Addresses Network Address Translation Overview on page 191</a></li></ul>

## match-direction

---

<b>Syntax</b>	match-direction (input   output);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the direction in which the rule match is applied.
<b>Options</b>	<b>input</b> —Apply the rule match on input. <b>output</b> —Apply the rule match on output.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## no-translation

---

<b>Syntax</b>	no-translation;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	Specify that traffic is not to be translated.
<b>Options</b>	none
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## overload-pool

---

<b>Syntax</b>	overload-pool <i>overload-pool-name</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then translated</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	Specify an address pool that can be used if the source pool becomes exhausted.
<b>Options</b>	<i>overload-pool-name</i> —Name of the overload pool.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## overload-prefix

---

<b>Syntax</b>	<code>overload-prefix <i>overload-prefix</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then translated</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	Specify the prefix that can be used if the source pool becomes exhausted.
<b>Options</b>	<i>overload-prefix</i> —Prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## pool

**Syntax** `pool nat-pool-name {`  
     `address ip-prefix</prefix-length>;`  
     `address-allocation round-robin;`  
     `address-range low minimum-value high maximum-value;`  
     `app-mapping-timeout app-mapping-timeout;`  
     `ei-mapping-timeout ei-mapping-timeout;`  
     `mapping-timeout mapping-timeout;`  
     `pgcp {`  
         `hint [ hint-strings ];`  
         `ports-per-session ports;`  
         `remotely-controlled;`  
     `}`  
     `port (automatic | range low minimum-value high maximum-value) {`  
         `preserve-parity;`  
         `preserve-range;`  
         `secured-port-block-allocation {`  
             `active-block-timeout timeout-seconds;`  
             `block-size block-size;`  
             `max-blocks-per-user max-blocks;`  
         `}`  
     `}`  
`}`

**Hierarchy Level** [edit [services](#) nat]

**Release Information** Statement introduced before Junos OS Release 7.4.  
**pgcp** statement added in Junos OS Release 8.4.  
**remotely-controlled** and **ports-per-session** statements added in Junos OS Release 8.5.  
**hint** statement added in Junos OS Release 9.0.  
**address-allocation** statement added in Junos OS Release 11.2.

**Description** Specify the NAT name and properties.

**Options** *nat-pool-name*—Identifier for the NAT address pool.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
 interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Pools of Addresses and Ports for Network Address Translation Overview on page 192](#)

## port

---

<b>Syntax</b>	<pre>port (automatic   range low <i>minimum-value</i> high <i>maximum-value</i> random-allocation) {   preserve-parity;   preserve-range;   deterministic-port-block-allocation &lt;block-size <i>block-size</i>&gt; &lt;include-boundary-addresses&gt;;   secured-port-block-allocation {     active-block-timeout <i>timeout-seconds</i>;     block-size <i>block-size</i>;     max-blocks-per-user <i>max-blocks</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> <i>nat-pool-name</i> ]
<b>Release Information</b>	<p><b>port</b> statement introduced before Junos OS Release 7.4.</p> <p><b>random-allocation</b> statement introduced in Junos OS Release 9.3.</p> <p><b>secured-port-block-allocation</b> statement introduced in Junos OS Release 11.2.</p> <p><b>deterministic-port-block-allocation</b> statement introduced in Junos OS Release 12.1.</p>
<b>Description</b>	Specify the NAT pool port or range. You can configure an automatically assigned port or specify a range with minimum and maximum values.
<b>Options</b>	<p><b>automatic</b>—Router-assigned port.</p> <p><b><i>minimum-value</i></b>—Lower boundary for the port range.</p> <p><b><i>maximum-value</i></b>—Upper boundary for the port range.</p> <p><b>preserve-parity</b>—Allocate ports with same parity as the original port.</p> <p><b>preserve-range</b>—Preserve privileged port range after translation.</p> <p><b>random-allocation</b>—Allocate ports within a specified range randomly.</p> <p>Other options are described separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Source and Destination Addresses Network Address Translation Overview on page 191</a></li><li>• <a href="#">Configuring Address Pools for Network Address Port Translation (NAPT) Overview on page 194</a></li></ul>

## port-forwarding

---

<b>Syntax</b>	<code>port-forwarding map-name {     destined-port;     translated-port; }</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Specify the mapping for port forwarding.
<b>Options</b>	<i>map-name</i> —Identifier for the port forwarding map.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port Forwarding for Static Destination Address Translation on page 251</a></li><li>• <a href="#">Configuring Port Forwarding Without Destination Address Translation on page 254</a></li></ul>

## port-forwarding-mappings

---

<b>Syntax</b>	<code>port-forwarding-mappings map-name;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> rule-name <a href="#">term</a> term-name then]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Specify the name for mapping port forwarding in a Network Address Translation configuration.
<b>Options</b>	<i>map-name</i> —Identifier for the port forwarding mapping.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port Forwarding for Static Destination Address Translation on page 251</a></li><li>• <a href="#">Configuring Port Forwarding Without Destination Address Translation on page 254</a></li></ul>

## ports-per-session

---

<b>Syntax</b>	<code>ports-per-session <i>ports</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> <i>nat-pool-name</i> pgcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure the number of ports required to support Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP), Real-Time Streaming Protocol (RTSP), and forward error correction (FEC) for voice and video flows on the Multiservices PIC.
<b>Options</b>	<i>number-of-ports</i> —Number of ports to enable: 2 or 4 for combined voice and video services. <b>Default:</b> 2
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface—control—To add this statement to the configuration.

## rule

```
Syntax  rule rule-name {
    match-direction (input | output);
    term term-name {
        from {
            application-sets set-name;
            applications [ application-names ];
            destination-address (address | any-unicast) <except>;
            destination-address-range low minimum-value high maximum-value <except>;
            source-address (address | any-unicast) <except>;
            source-address-range low minimum-value high maximum-value <except>;
        }
        then {
            no-translation;
            translated {
                address-pooling paired;
                destination-pool nat-pool-name;
                destination-prefix destination-prefix; destination-prefix;
                dns-alg-pool dns-alg-pool;
                dns-alg-prefix dns-alg-prefix;
                filtering-type endpoint-independent;
                mapping-type endpoint-independent;
                overload-pool overload-pool;
                overload-prefix overload-prefix;
                source-pool nat-pool-name;
                source-prefix source-prefix;
                translation-type (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | dynamic-nat44
                    | napt-44 | napt-66 | napt-pt | stateful-nat64 | twice-basic-nat-44 |
                    twice-dynamic-nat-44 | twice-napt-44);
            }
        }
        syslog;
    }
}
```

**Hierarchy Level** [edit [services nat](#)],  
[edit [services nat rule-set rule-set-name](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Specify the rule the router uses when applying this service.



**NOTE:** You are limited to a maximum of 200 terms for a NAT rule that is applied to an inline services (type si) interface. If you specify more than 200 terms, you will receive following error when you commit the configuration:

```
[edit]
' service-set service-set-name'
  NAT rule rule-name with more than 200 terms is disallowed for
  si-n/n.n.n
error: configuration check-out failed
```

<b>Options</b>	<i>rule-name</i> —Identifier for the collection of terms that make up this rule.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

---

## rule-set

<b>Syntax</b>	<pre>rule-set <i>rule-set-name</i> {     [ <i>rule</i> <i>rule-names</i> ]; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<i>rule-set-name</i> —Identifier for the collection of rules that constitute this rule set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

---

## secure-nat-mapping

<b>Syntax</b>	<pre>secure-nat-mapping {     <i>mapping-refresh</i> (inbound   outbound   inbound-outbound);     <i>if-flow-limit</i> <i>number-of-flows</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <i>rule</i> <i>rule-name</i> <i>term</i> <i>term-name</i> <i>then translated</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3
<b>Options</b>	The statements are explained separately.  —
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>•</li></ul>

## secured-port-block-allocation

<b>Syntax</b>	secured-port-block-allocation { active-block-timeout <i>timeout-seconds</i> ; block-size <i>block-size</i> ; max-blocks-per-address <i>max-blocks</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">pool</a> <i>pool-name</i> port]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	When you use block allocation, one or more blocks of ports in a NAT pool address range are available for assignment to a subscriber.
<b>Options</b>	<p><b><i>block-size</i></b>—Number of ports included in a block.  <b>Default:</b> 128  <b>Range:</b> 1 to 32,000</p> <p><b><i>max-blocks</i></b>—Maximum number of blocks that can be allocated to a user address.  <b>Default:</b> 8  <b>Range:</b> 1 to 512</p> <p><b><i>timeout-seconds</i></b>—Interval, in seconds, during which a block is active. After timeout, a new block is allocated, even if ports are available in the active block.  <b>Default:</b> 0—The default timeout of the active block is 0 (infinite). In this case, the active block transitions to inactive only when it runs out of ports and a new block is allocated. Any inactive block without any ports in use will be freed to the NAT pool.  <b>Range:</b> Any value greater than or equal to 120.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Address Pools for Network Address Port Translation (NAPT) Overview on page 194</a></li> </ul>

## server (pcp)

---

**Syntax**    `server server-name {  
                ipv4-address ipv4-address;  
                ipv6-address ipv6-address;  
                software-concentrator software-concentrator-name;  
                mapping-lifetime-min mapping-lifetime-min;  
                mapping-lifetime-max mapping-lifetime-max;  
                short-lifetime-error short-lifetime-error;  
                long-lifetime-error long-lifetime-error;  
                nat-options {  
                    pool pool-name ;  
                }  
                pcp-options {  
                    third-party  
                    prefer-failure  
                }  
                max-mapping-per-client max-mapping-per-client;  
            }`

**Hierarchy Level**    [edit services pcp]

**Release Information**    Statement introduced in Junos OS Release 13.2R1.

**Description**    Configure PCP server options.

**Options**    *ipv4-address*—IPv4 address of the PCP server.

*ipv6-address*—IPv6 address of the PCP server.

*software-concentrator-name*—Software concentrator name whose software-address is used in creating PCP mappings. The PCP server address must be the same as the software-concentrator address.

*mapping-lifetime-min*—Minimum lifetime, in seconds, for PCP mapping. If a PCP client requests a lifetime less than the minimum configured, the server will assign a minimum lifetime and respond accordingly.

**Default:** 300 seconds

**Range:** 120 through 3600 seconds

*mapping-lifetime-max mapping-lifetime-max*—Maximum lifetime, in seconds, for PCP mapping. If the PCP client requests a lifetime less than the maximum configured, the server will assign the maximum lifetime and respond accordingly.

**Default:** 86,400 seconds

**Range:** 3600 through 2147483647 seconds

*short-lifetime-error short-lifetime-error*—Certain error opcodes mentioned in section 2 are classified as short lifetime errors. In case of these errors, the PCP server will use the value configured with this option to respond to the PCP client.

**Default:** 30 seconds

**Range:** 15 through 300 seconds

***long-lifetime-error***—Certain error opcodes mentioned in section 2 are classified as long lifetime errors. In case of these errors, the PCP server will use the value configured with this option to respond to the PCP client.

**Default:** 1800 seconds

**Range:** 900 through 18,000 seconds

***max-mapping-per-client number-of-mappings***—Maximum number of PCP mappings that the PCP client can request.

**Default:** 32

**Range:** 1 through 32

The other statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Port Control Protocol on page 257](#)

---

## services (NAT)

---

**Syntax** services nat { ... }

**Hierarchy Level** [edit]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the service rules to be applied to traffic.

**Options** nat—Identifies the NAT set of rules statements.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

## service-set (Services)

```
Syntax  service-set service-set-name {
        allow-multicast;
        extension-service service-name {
            provider-specific-rules-configuration;
        }
        (ids-rules rule-name | ids-rule-sets rule-set-name);
        interface-service {
            service-interface interface-name;
        }
        ipsec-vpn-options {
            anti-replay-window-size bits;
            clear-dont-fragment-bit;
            ike-access-profile profile-name;
            local-gateway address;
            no-anti-replay;
            passive-mode-tunneling;
            trusted-ca [ ca-profile-names ];
            tunnel-mtu bytes;
        }
        ip-reassembly-rules rule-name;
        (ipsec-vpn-rules rule-name | ipsec-vpn-rule-sets rule-set-name);
        max-flows number;
        max-drop-flows {
            ingress ingress-flows;
            egress egress-flows;
        }
        nat-options {
            land-attack-check (ip-only | ip-port);
            max-sessions-per-subscriber session-number;
            stateful-nat64 {
                clear-dont-fragment-bit;
            }
        }
        (nat-rules rule-name | nat-rule-sets rule-set-name);
        next-hop-service {
            inside-service-interface interface-name.unit-number;
            outside-service-interface interface-name.unit-number;
            outside-service-interface-type local;
            service-interface-pool name;
        }
        (pgcp-rules rule-name | pgcp-rule-sets rule-set-name);
        (ptsp-rules rule-name | ptsp-rule-sets rule-set-name);
        service-set-options {
            bypass-traffic-on-exceeding-flow-limits;
            bypass-traffic-on-pic-failure;
            enable-asymmetric-traffic-processing;
            support-uni-directional-traffic;
        }
        snmp-trap-thresholds {
            flows high high-threshold | low low-threshold;
            nat-address-port high-threshold | low low-threshold;
        }
    }
```

```

}
software-options {
  dslite-ipv6-prefix-length dslite-ipv6-prefix-length;
}
(software-rules rule-name | software-rule-sets rule-set-name);
(stateful-firewall-rules rule-name | stateful-firewall-rule-sets rule-set-name);
syslog {
  host hostname {
    class {
      alg-logs;
      ids-logs;
      nat-logs;
      packet-logs;
      pcp-logs;
      session-logs <open | close>;
      stateful-firewall-logs ;
    }
    services severity-level;
    facility-override facility-name;
    interface-service prefix-value;
  }
}
}

```

Hierarchy Level	[edit services]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p><b>pgcp-rules</b> and <b>pgcp-rule-sets</b> options added in Junos OS Release 8.4.</p> <p><b>server-set-options</b> option added in Junos OS Release 10.1.</p> <p><b>ptsp-rules</b> and <b>ptsp-rule-sets</b> options added in Junos OS Release 10.2.</p> <p><b>software-rules</b> and <b>clear-rule-sets</b> options added in Junos OS Release 10.4.</p> <p><b>software-options</b> option added in Junos OS Release 14.1.</p>
Description	Define the service set.
Options	<p><b><i>service-set-name</i></b>—Name of the service set.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <li><i>Service Set Properties</i></li> </ul>

## source-address (NAT)

---

Syntax	source-address ( <i>address</i>   any-unicast) <except>;
Hierarchy Level	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
Release Information	Statement introduced before Junos OS Release 7.4. <b>any-unicast</b> and <b>except</b> options introduced in Junos OS Release 7.6. <b>address</b> option enhanced to support IPv6 addresses in Junos OS Release 8.5.
Description	Specify the source address for rule matching.
Options	<b>address</b> —Source IPv4 or IPv6 address or prefix value. <b>any-unicast</b> —Any unicast packet. <b>except</b> —(Optional) Prevent the specified address or unicast packets from being translated.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## source-address-range

---

Syntax	source-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>;
Hierarchy Level	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
Release Information	Statement introduced in Junos OS Release 7.6. <b>minimum-value</b> and <b>maximum-value</b> options enhanced to support IPv6 addresses in Junos OS Release 8.5.
Description	Specify the source address range for rule matching.
Options	<b>minimum-value</b> —Lower boundary for the IPv4 or IPv6 address range. <b>maximum-value</b> —Upper boundary for the IPv4 or IPv6 address range. <b>except</b> —(Optional) Prevent the specified address range from being translated.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## source-pool

---

<b>Syntax</b>	<code>source-pool nat-pool-name;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then translated</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the source address pool for translated traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## source-prefix

---

<b>Syntax</b>	<code>source-prefix source-prefix;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then translated</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6. <i>source-prefix</i> option enhanced to support IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Specify the source prefix for translated traffic.
<b>Options</b>	<i>source-prefix</i> —IPv4 or IPv6 source prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## source-prefix-list

---

<b>Syntax</b>	source-prefix-list <i>list-name</i> <except>;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	Specify the source prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the <a href="#">[edit policy-options]</a> hierarchy level.
<b>Options</b>	<i>list-name</i> —Destination prefix list.  <b>except</b> —(Optional) Exclude the specified prefix list from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li><li>• <a href="#">Routing Policy Feature Guide for Routing Devices</a></li></ul>

## syslog

---

<b>Syntax</b>	syslog;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Enable system logging. The system log information from the Multiservices PIC is passed to the kernel for logging in the <b>/var/log</b> directory.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

## translated-port

---

<b>Syntax</b>	<code>translated-port <i>port id</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> nat <a href="#">port-forwarding</a> <i>map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Specify the port to which all traffic will be translated.
<b>Options</b>	<i>port id</i> —The port number to which traffic will be translated.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">port-forwarding on page 325</a></li><li>• <a href="#">destined-port on page 314</a></li></ul>

## term

```
Syntax  term term-name {
        from {
            application-sets set-name;
            applications [ application-names ];
            destination-address (address | any-unicast) <except>;
            destination-address-range low minimum-value high maximum-value <except>;
            source-address (address | any-unicast) <except>;
            source-address-range low minimum-value high maximum-value <except>;
        }
        then {
            no-translation;
            translated {
                address-pooling paired;
                destination-pool nat-pool-name;
                destination-prefix destination-prefix;
                dns-alg-pool dns-alg-pool;
                dns-alg-prefix dns-alg-prefix;
                filtering-type endpoint-independent;
                mapping-type endpoint-independent;
                source-pool nat-pool-name;
                source-prefix source-prefix;
                translation-type (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | dynamic-nat44
                    | napt-44 | napt-66 | napt-pt | stateful-nat64 | twice-basic-nat-44 |
                    twice-dynamic-nat-44 | twice-napt-44);
            }
        }
        syslog;
    }
```

**Hierarchy Level** [edit [services](#) nat [rule](#) *rule-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the NAT term properties.

**Options** *term-name*—Identifier for the term.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Network Address Translation Rules Overview on page 204](#)

## then

```
Syntax  then {
        no-translation;
        translated {
            address-pooling paired;
            destination-pool nat-pool-name;
            destination-prefix destination-prefix;
            dns-alg-pool dns-alg-pool;
            dns-alg-prefix dns-alg-prefix;
            filtering-type endpoint-independent;
            mapping-type endpoint-independent;
            source-pool nat-pool-name;
            source-prefix source-prefix;
            translation-type (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | dynamic-nat44
                            | napt-44 | napt-66 | napt-pt | stateful-nat64 | twice-basic-nat-44 |
                            twice-dynamic-nat-44 | twice-napt-44);
        }
    }
    syslog;
}
```

**Hierarchy Level** [edit [services](#) nat [rule](#) *rule-name* [term](#) *term-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the NAT term actions.

**Options** The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Network Address Translation Rules Overview on page 204](#)

## translated

---

**Syntax**    translated {  
             address-pooling paired;  
             destination-pool *nat-pool-name*;  
             destination-prefix *destination-prefix*;  
             dns-alg-pool *dns-alg-pool*;  
             dns-alg-prefix *dns-alg-prefix*;  
             filtering-type endpoint-independent;  
             mapping-type endpoint-independent;  
             overload-pool *overload-pool-name*;  
             overload-prefix;  
             source-pool *nat-pool-name*;  
             translation-type (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | dynamic-nat44 |  
                              napt-44 | napt-66 | napt-pt | stateful-nat64 | twice-basic-nat-44 | twice-dynamic-nat-44  
                              | twice-napt-44)  
             }  
             }

**Hierarchy Level**    [edit [services](#) nat [rule](#) *rule-name* [term](#) *term-name* [then](#)]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Define properties for translated traffic.

**Options**    The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • [Network Address Translation Rules Overview on page 204](#)

## translation-type

<b>Syntax</b>	translation-type (basic-nat-pt   basic-nat44   basic-nat66   nat-44   deterministic-napt44   dnat-44   dynamic-nat44   napt-44   napt-66   napt-pt   stateful-nat64   twice-basic-nat-44   twice-dynamic-nat-44   twice-napt-44)
<b>Hierarchy Level</b>	[edit <b>services</b> nat <b>rule</b> <i>rule-name</i> <b>term</b> <i>term-name</i> <b>then</b> translated]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>The following options introduced in Junos OS Release 11.2, replacing all previous options:</p> <ul style="list-style-type: none"> <li>• <b>basic-nat44</b></li> <li>• <b>basic-nat66</b></li> <li>• <b>basic-nat-pt</b></li> <li>• <b>deterministic-napt44</b></li> <li>• <b>dnat-44</b></li> <li>• <b>dynamic-nat44</b></li> <li>• <b>napt-44</b></li> <li>• <b>napt-66</b></li> <li>• <b>napt-pt</b></li> <li>• <b>stateful-nat64</b></li> </ul> <p><b>twice-basic-nat-44</b> option introduced in Junos OS Release 11.4.</p> <p><b>twice-dynamic-nat-44</b> option introduced in Junos OS Release 11.4.</p> <p><b>twice-napt-44</b> option introduced in Junos OS Release 11.4.</p> <p><b>deterministic-napt44</b> option introduced in Junos OS Release 12.1.</p>
<b>Description</b>	Specify the NAT translation types.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>basic-nat44</b>—Translate the source address statically (IPv4 to IPv4).</li> <li>• <b>basic-nat66</b>—Translate the source address statically (IPv6 to IPv6).</li> <li>• <b>basic-nat-pt</b>—Translate the addresses of IPv6 hosts as they originate sessions to the IPv4 hosts in the external domain. The <b>basic-nat-pt</b> option is always implemented with DNS ALG.</li> <li>• <b>deterministic-napt44</b>—Translate as <b>napt-44</b>, and use deterministic port block allocation for port translation.</li> <li>• <b>dnat-44</b>—Translate the destination address statically (IPv4 to IPv4).</li> <li>• <b>dynamic-nat44</b>—Translate only the source address by dynamically choosing the NAT address from the source address pool.</li> </ul>

- **napt-44**—Translate the transport identifier of the IPv4 private network to a single IPv4 external address.
- **napt-66**—Translate the transport identifier of the IPv6 private network to a single IPv6 external address.
- **napt-pt**—Bind addresses in an IPv6 network with addresses in an IPv4 network and vice versa to provide transparent routing for the datagrams traversing between the address realms.
- **stateful-nat64**—Implement dynamic address and port translation for source IP addresses (IPv6-to-IPv4) and prefix removal translation for the destination IP addresses (IPv6-to-IPv4).
- **twice-basic-nat-44**—Translate the source and destination addresses statically (IPv4 to IPv4).
- **twice-dynamic-nat-44**—Translate the source address by dynamically choosing the NAT address from the source address pool. Translate the destination address statically.
- **twice-dynamic-napt-44**—Translate the transport identifier of the IPv4 private network to a single IPv4 external address. Translate the destination address statically.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Network Address Translation Rules Overview on page 204</a></li></ul>

# Softwire Configuration Guidelines

- [Configuring a DS-Lite Softwire Concentrator on page 343](#)
- [Configuring a 6rd Softwire Concentrator on page 344](#)
- [Configuring Stateful Firewall Rules for 6rd Softwire on page 345](#)
- [Configuring Softwire Rules on page 345](#)
- [Configuring Service Sets for Softwire on page 346](#)
- [Example: Basic DS-Lite Configuration on page 347](#)
- [Example: Basic 6rd Configuration on page 353](#)
- [Example: Configuring DS-Lite and 6rd in the Same Service Set on page 358](#)
- [Configuring a 6to4 Provider-Managed Tunnel on page 364](#)

## Configuring a DS-Lite Softwire Concentrator

---

To configure a DS-Lite softwire concentrator:

1. Assign a name to the DS-Lite softwire concentrator.

```
[edit services softwire softwire-concentrator]
user@host# edit ds-lite ds-lite-softwire-concentrator
```

2. Specify the address of the softwire tunnel.

```
[edit services softwire softwire-concentrator ds-lite ds-lite-softwire-concentrator]
user@host# set softwire-address address
```

3. Specify the MTU for the softwire tunnel.

```
[edit services softwire softwire-concentrator ds-lite ds-lite-softwire-concentrator]
user@host# set mtu-v6 mtu-v6
```



**NOTE:** This option sets the maximum transmission unit when encapsulating IPv4 packets into IPv6. If the final length is greater than the MTU, the IPv6 packet will be fragmented. This option is mandatory since it depends on other network parameters under administrator control.

4. To copy DSCP information from the IPv6 header into the decapsulated IPv4 header, include the **copy-dscp** statement.

```
[edit services software software-concentrator ds-lite ds-lite-software-concentrator]  
user@host# set copy-dscp
```

5. Specify the maximum number of flows for the software

```
[edit services software software-concentrator ds-lite ds-lite-software-concentrator]  
user@host# set flow-limit 1000
```

**Related  
Documentation**

- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 71](#)
- [Configuring Software Rules on page 345](#)
- [Configuring IPv6 Multicast Interfaces](#)
- [Configuring Service Sets for Software on page 346](#)
- [Example: Basic DS-Lite Configuration on page 347](#)
- [Example: Configuring DS-Lite and 6rd in the Same Service Set on page 358](#)

---

## Configuring a 6rd Software Concentrator

---

To configure a 6rd software concentrator:

1. Assign a name to the 6rd software concentrator.

```
[edit services software software-concentrator]  
user@host# edit v6rd v6rd-software-concentrator
```

2. Specify the address of the software tunnel.

```
[edit services software software-concentrator v6rd v6rd-software-concentrator]  
user@host# set software-address address
```

3. Specify the MTU for the software tunnel.

```
[edit services software software-concentrator v6rd v6rd-software-concentrator]  
user@host# set mtu-v4 mtu-v4
```



**TIP:** In this release there is no support for fragmentation and reassembly, therefore the MTUs on the IPv6 and IPV4 network must be properly configured by the administrator.

---

**Related  
Documentation**

- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 71](#)
- [Configuring Software Rules on page 345](#)
- [Configuring Stateful Firewall Rules for 6rd Software on page 345](#)
- [Configuring Service Sets for Software on page 346](#)
- [Example: Basic 6rd Configuration on page 353](#)
- [Example: Configuring DS-Lite and 6rd in the Same Service Set on page 358](#)

## Configuring Stateful Firewall Rules for 6rd Software

You must configure a stateful firewall rule for use with 6rd softwires. The stateful firewall service is used only to direct packets to the software, not for firewalling purposes. The 6rd software service itself must be stateless. To support stateless processing, you must include an **allow** term in both directions of the stateful firewall policy.

To include a stateful firewall rule for 6rd software processing:

1. Assign a name to the rule.

```
[edit services stateful-firewall]
user@host# edit rule rule-name
```

2. Specify the match direction.

```
[edit services stateful-firewall rule-name]
user@host# set match-direction input-output
```

3. Assign a name for the term.

```
[edit services stateful-firewall rule-name]
user@host# edit term term-name
```

4. Specify that all traffic in both directions should be accepted for the software process.

```
[edit services stateful-firewall rule-name term term-name]
user@host# set then accept
```

### Related Documentation

- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 71](#)
- [Configuring a 6rd Software Concentrator on page 344](#)
- [Configuring Software Rules on page 345](#)
- [Configuring Service Sets for Software on page 346](#)
- [Example: Basic 6rd Configuration on page 353](#)
- [Example: Configuring DS-Lite and 6rd in the Same Service Set on page 358](#)

## Configuring Software Rules

You configure software rules to instruct the router how to direct traffic to the addresses specified for 6rd or DS-Lite software concentrators. Software rules do not perform any filtration of the traffic. They do not include a **from** statement, and the only option in the **then** statement is to specify the address of the 6rd or DS-Lite software concentrator.

You can create a software rule consisting of one or more terms and associate a particular 6rd or DS-Lite software concentrator with each term. You can include the software rule in service sets along with other services rules.

To configure a software rule:

1. Assign a name to the rule.

```
[edit services software ]
user@host# edit rule rule-name
```

2. Specify the match direction.

```
[edit services software rule rule-name]
user@host# set match-direction (input | output)
```

3. Assign a name for the first term.

```
[edit services software rule rule-name]
user@host# edit term term-name
```

4. Associate a 6rd or DS-Lite software concentrator with this term.

```
[edit services software rule rule-name term term-name]
user@host# set then ds-lite name
```

Or

```
user@host# set then v6rd v6rd-software-concentrator
```

5. Repeat Steps 3 and 4 for as many additional terms as needed.

#### Related Documentation

- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 71](#)
- [Configuring a 6rd Software Concentrator on page 344](#)
- [Configuring a DS-Lite Software Concentrator on page 343](#)
- [Configuring IPv6 Multicast Interfaces](#)
- [Configuring Service Sets for Software on page 346](#)

---

## Configuring Service Sets for Software

You must include software rules or a software rule set in a service set to enable software processing. You must include a stateful firewall rule for DS-Lite.

To configure service sets for software:

1. Include a software rule or rule set in the service set.

```
[edit services service-set service-set-name]
user@host# set software-rules rule software-rule-name
```

2. When using a 6rd software, include a stateful-firewall rule.

```
[edit services service-set service-set-name]
user@host# set stateful-firewall-rules software-rule-name
```

3. You can include a NAT rule for flows originated by DS-Lite softwares.

**NOTE:**

Currently a NAT rule configuration is required with a DS-Lite software configuration when you use interface service set configurations; NAT is not required when using next-hop service set configurations. NAT processing from IPv4 to IPv6 address pools and vice versa is not currently supported. FTP, HTTP, and RSTP are supported.



**NOTE:** With a DS-Lite software concentrator, if you configure stateful firewall rules without configuring NAT rules, using an interface service set causes the ICMP echo reply messages to be not sent correctly to DS-Lite. This behavior occurs if you apply a service set to both inet and inet6 families. In such a scenario, the traffic that is not destined to the DS-Lite software concentrator is also processed by the service set and the packets might be dropped, although the service set must not process such packets.

To prevent the problem to incorrect processing of traffic applicable for DS-Lite, you must configure a next-hop style service set and not an interface style service set. This problem does not occur when you configure NAT rules with interface service sets for DS-Lite.

For further information, see [“Configuring Service Rules” on page 747.](#)

**Related Documentation**

- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 71](#)
- [Configuring Software Rules on page 345](#)
- [Example: Configuring DS-Lite and 6rd in the Same Service Set on page 358](#)

## Example: Basic DS-Lite Configuration

- [Requirements on page 347](#)
- [Configuration Overview and Topology on page 348](#)
- [Configuration on page 348](#)

## Requirements

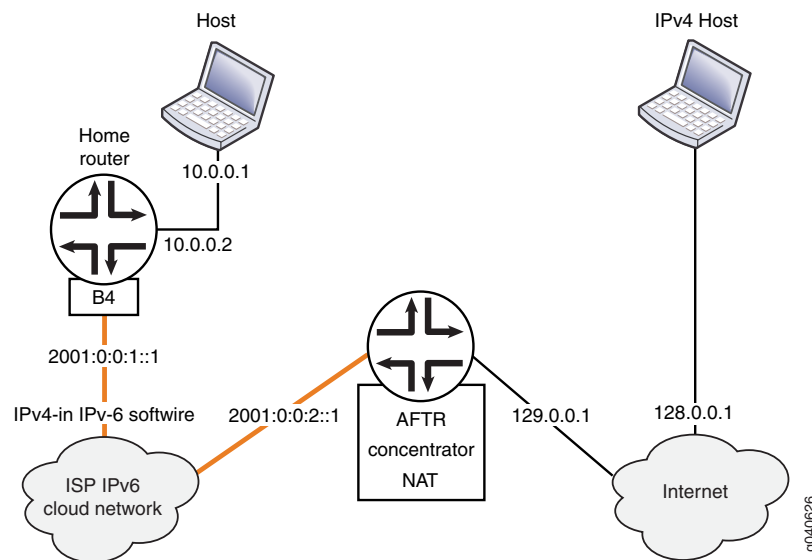
The following hardware components can perform DS-Lite:

- M Series Multiservice Edge routers with Multiservices PICs
- T Series Core routers with Multiservices PICs
- MX Series 3D Universal Edge routers with Multiservices DPCs

## Configuration Overview and Topology

This example describes how to configure an MX Series router with an MS-DPC as an AFTR to facilitate the flow shown in [Figure 16 on page 348](#).

**Figure 16: DS-Lite Topology**



In this example, the DS-Lite software concentrator, or AFTR, is an MX Series router with two Gigabit interfaces and a Services DPC. The interface facing the B4 element is ge-3/1/5 and the interface facing the Internet is ge-3/1/0.

## Configuration

- [Chassis Configuration on page 348](#)
- [Interfaces Configuration on page 349](#)
- [Network Address and Port Translation Configuration on page 350](#)
- [Software Configuration on page 351](#)
- [Service Set Configuration on page 352](#)

### Chassis Configuration

#### Step-by-Step Procedure

To configure the service PIC (FPC 0 Slot 0) with the Layer 3 service package:

1. Enter the **edit chassis** hierarchy level.  

```
user@host# edit chassis
```
2. Configure the Layer 3 service package.  

```
[edit chassis]
user@host# set fpc 0 pic 0 adaptive-services service-package layer-3
```

## Interfaces Configuration

- Step-by-Step Procedure** interfaces facing the B4 (software initiator) and facing the Internet:
1. Go to the **[edit interfaces]** edit hierarchy level for ge-3/1/0, which faces the Internet.  

```
host# edit interfaces ge-3/1/0
```
  2. Define the interface.  

```
[edit interfaces ge-3/1/0]
user@host# set description AFTR-Internet
user@host# set unit 0 family inet address 128.0.0.2/24
```
  3. Go to the **[edit interfaces]** hierarchy level for ge-3/1/5, which faces the B4.  

```
user@host# up 1
[edit]
user@host# edit interfaces ge-3/1/5
```
  4. Define the interface.  

```
[edit interfaces ge-3/1/5]
user@host# set description AFTR-B4
user@host# set unit 0 family inet
user@host# edit unit 0 family inet6
[edit unit 0 family inet6]
user@host# set service input service-set sset
user@host# set service output service-set sset
user@host# set address 2001:0:0:2::1/48
```
  5. Go to the **[edit interfaces]** hierarchy level for sp-0/0/0, used to host the DS-Lite AFTR.  

```
[edit]
user@host# edit interfaces sp-0/0/0
```
  6. Define the interface.  

```
[edit interfaces sp-0/0/0]
user@host# set description AFTR-B4
user@host# set unit 0 family inet
user@host# edit unit 0 family inet6
```

**Results**

```
user@host# show interfaces ge-3/1/0
description AFTR-Internet;
unit 0 {
    family inet {
        address 128.0.0.2/24;
    }
}

user@host# show interfaces ge-3/1/5
description AFTR-B4;
unit 0 {
    family inet;
    family inet6 {
        service {
            input {
                service-set sset;
            }
            output {
                service-set sset;
            }
        }
        address 2001:0:0:2::1/48;
    }
}

user@host# show interfaces sp-o/o/o
unit 0 {
    family inet;
    family inet6;
}
```

---

### Network Address and Port Translation Configuration

#### Step-by-Step Procedure

To configure NAPT:

1. Go to the **[edit services nat]** hierarchy level.  

```
user@host# edit services nat
[edit services nat]
```
2. Define a NAT pool p1.  

```
user@host# set pool p1 address 129.0.0.1/32 port automatic
```
3. Define a NAT rule, beginning with the match direction.  

```
[edit services nat]
user@host# set rule r1 match-direction input
```
4. Define a **term** for the rule, beginning with a from clause.  

```
[edit services nat]
user@host# set rule r1 term t1 from source-address 10.0.0.0/16
```
5. Define the desired translation in a **then** clause. In this case, use dynamic source translation.  

```
[edit services nat]
user@host# set rule r1 term t1 then translated source-pool p1 translation-type napt-44
```
6. (Optional) Configure logging of translation information for the rule.

```
[edit services nat]
user@host# set rule r1 term t1 then syslog
```

**Results**

```
user@host# show services nat
pool p1 {
  address 129.0.0.1/32;
  port {
    automatic;
  }
}
rule r1 {
  match-direction input;
  term t1 {
    from {
      source-address {
        10.0.0.0/16;
      }
    }
    then {
      translated {
        source-pool p1;
        translation-type {
          napt-44;
        }
      }
      syslog;
    }
  }
}
```

### Software Configuration

**Step-by-Step Procedure** To configure the DS-Lite software concentrator and associated rules:

1. Go to the **[edit services software]** hierarchy level.  

```
user@host# edit services software
```
2. Define the DS-Lite software concentrator.  

```
[edit services software]
user@host# set software-concentrator ds-lite ds-1 software-address 1001::1 mtu-v6 1460
```
3. Define the software rule.  

```
[edit services software]
user@host# set rule r1 match-direction input term t1 then ds-lite ds1.
```

**Results**    `user@host# show services software`

```
software-concentrator {
  ds-lite ds1 {
    software-address 1001::1;
    mtu-v6 1460;
  }
}
rule r1 {
  match-direction input;
  term t1 {
    then {
      ds-lite ds1;
    }
  }
}
```

---

### Service Set Configuration

**Step-by-Step Procedure**    Configure a service set that includes software and NAT rules and specifies either interface-service or next-hop service. This example uses a next-hop service.

1. Go to the `[edit services service-set]` hierarchy level, naming the service set.

```
user@host# edit services service-set sset
```

2. Define the NAT rule to be used for IPv4-to-IPv4 translation.

```
[edit services service-set sset]
user@host# set nat-rules r1
```

3. Define the software rule to define the software tunnel.

```
[edit services service-set sset]
user@host# set software-rules r1
```

4. Define the interface service,

```
[edit services service-set sset]
user@host# set interface-service service-interface sp-0/0/0.0
```



**TIP:** In order to avoid or minimize IPv6 fragmentation, you can configure a TCP maximum segment size (MSS) for your service set.

---

5. (Optional) Define a TCP MSS.

```
[edit services service-set sset]
user@host# set tcp-mss 1024
```

**Results** `user@host# show services service-set`

```

syslog {
  host local {
    services any;
  }
}
software-rules r1;
nat-rules r1;
interface-service {
  service-interface sp-0/0/0;
}
}

```

- Related Documentation**
- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 71](#)
  - [Configuring a DS-Lite Software Concentrator on page 343](#)
  - [Configuring Software Rules on page 345](#)
  - [Configuring Service Sets for Software on page 346](#)
  - [Example: Basic 6rd Configuration on page 353](#)
  - [Example: Configuring DS-Lite and 6rd in the Same Service Set on page 358](#)

## Example: Basic 6rd Configuration

- [Requirements on page 353](#)
- [Overview on page 353](#)
- [Configuration on page 353](#)

### Requirements

This example describes how a 6rd concentrator can be configured for a 6rd domain, D1, to provide IPv6 Internet connectivity.

The following hardware components can perform 6rd:

- M Series Multiservice Edge routers with Multiservices PICs
- T Series Core routers with Multiservices PICs
- MX Series 3D Universal Edge routers with Multiservices DPCs

### Overview

This configuration example describes how to configure a basic 6rd tunneling solution.

### Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set interfaces ge-1/2/0 unit 0 family inet service input service-set v6rd-dom1-service-set
set interfaces ge-1/2/0 unit 0 family inet service output service-set v6rd-dom1-service-set
set interfaces ge-1/2/0 unit 0 family inet address 10.10.10.1/24
set interfaces ge-1/2/0 unit 0 family inet6 service input service-set v6rd-dom1-service-set
set interfaces ge-1/2/0 unit 0 family inet6 service output service-set v6rd-dom1-service-set
set interfaces ge-1/2/2 unit 0 family inet6 address 3abc::1/16
set interfaces sp-0/2/0 unit 0 family inet
set interfaces sp-0/2/0 unit 0 family inet6
set services software software-concentrator v6rd v6rd-dom1 software-address 30.30.30.1
set services software software-concentrator v6rd v6rd-dom1 ipv4-prefix 10.10.10.0/24
set services software software-concentrator v6rd v6rd-dom1 v6rd-prefix 3040::0/16
set services software software-concentrator v6rd v6rd-dom1 mtu-v4 9192
set services software rule v6rd-dom1 match-direction input
set services software rule v6rd-dom1 term t1 then v6rd v6rd-dom1
set services service-set v6rd-dom1-service-set software-rules v6rd-dom1
set services service-set v6rd-dom1-service-set stateful-firewall-rules r1
set services service-set v6rd-dom1-service-set interface-service service-interface sp-0/2/0
set services stateful-firewall rule r1 match-direction input-output
set services stateful-firewall rule r1 term t1 then accept
```

---

### Chassis Configuration

#### Step-by-Step Procedure

To configure the chassis:

1. Define the ingress interface.  

```
user@host# edit interfaces ge-1/2/0
```
2. Configure the ingress interface logical unit and input/output service options.  

```
[edit interfaces ge-1/2/0]
user@host# set unit 0 family inet service input service-set v6rd-dom1-service-set
user@host# set unit 0 family inet service output service-set v6rd-dom1-service-set
user@host# set unit 0 family inet6 service input service-set v6rd-dom1-service-set
user@host# set unit 0 family inet6 service output service-set v6rd-dom1-service-set
```
3. Configure the address of the ingress interface.  

```
[edit interfaces ge-1/2/0]
user@host# set unit 0 family inet address 10.10.10.1/24
```
4. Define the egress interface.  

```
user@host# up
[edit interfaces]
user@host# edit ge-1/2/2
```
5. Define the logical unit and address for the egress interface.  

```
[edit interfaces ge-1/2/2]
user@host# set unit 0 family inet6 address 3ABC::1/16
```
6. Define the services PIC.  

```
[edit interfaces ge-1/2/2]
user@host# up
[edit interfaces]
user@host# edit sp-0/2/0
```
7. Configure the logical unit for the services PIC.

```
[edit interfaces sp-0/2/0]
user@host# up
[edit interfaces]
user@host# set unit 0 family inet
user@host# set unit 0 family inet6
```

**Results**

```
[edit interfaces]
user@router# show
sp-0/2/0 {
  unit 0 {
    family inet;
    family inet6;
  }
}
ge-1/2/0 {
  unit 0 {
    family inet {
      service {
        input {
          service-set v6rd-dom1-service-set;
        }
        output {
          service-set v6rd-dom1-service-set;
        }
      }
      address 10.10.10.1/24;
    }
    family inet6 {
      service {
        input {
          service-set v6rd-dom1-service-set;
        }
        output {
          service-set v6rd-dom1-service-set;
        }
      }
    }
  }
}
ge-1/2/2 {
  unit 0 {
    family inet6 {
      address 3abc::1/16;
    }
  }
}
```

### Software Concentrator, Software Rule, and Stateful Firewall Rule Configuration

**Step-by-Step Procedure** To configure the software concentrator, software rule, and stateful firewall rule:

1. Define the 6rd software concentrator.

```
user@host# top
user@host# edit services software software-concentrator v6rd v6rd-dom1
```

2. Configure the software concentrator properties. Here, software address 30.30.30.1 is the software concentrator IPv4 address, 10.10.10.0/24 is the IPv4 prefix of the CE WAN side, and 3040::0/16 is the IPv6 prefix of the 6rd domain D1.

```
[edit services software software-concentrator v6rd v6rd-dom1]
user@host# set software-address 30.30.30.1
user@host# set ipv4-prefix 10.10.10.0/24
user@host# set v6rd-prefix 3040::0/16
user@host# set mtu-v4 9192
```

3. Define the software rule.

```
[edit services software software-concentrator v6rd v6rd-dom1]
user@host# up 2
[edit services software]
user@host# edit rule v6rd-dom1
[edit services software rule v6rd-dom1]
user@host# set match-direction input
[edit services software rule v6rd-dom1]
user@host# set term t1 then v6rd v6rd-dom1
```

4. Define a stateful firewall rule and properties. You must configure a stateful firewall rule that accepts all traffic in both the input and output direction in order for 6rd to work; however, this is not enforced through the CLI. This is because in IPv6, gratuitous IPv6 packets are expected (due to Anycast) and should not be dropped. The service PIC can handle reverse traffic without seeing all forward traffic. This can also happen with service PIC switchover in the middle of a session. By default, the stateful firewall on the service PIC will drop all traffic unless a rule is configured explicitly to allow it.

```
[edit services software software-concentrator v6rd v6rd-dom1]
user@host# up 3
[edit services]
user@host# edit services stateful-firewall
[edit services stateful-firewall]
user@host# edit rule r1
[edit services stateful-firewall rule r1]
user@host# set match-direction input-output
user@host# set term t1 then accept
```

**Results** [edit services softwire]  
 user@router# show  
 softwire-concentrator {  
   v6rd v6rd-dom1 {  
     softwire-address 30.30.30.1;  
     ipv4-prefix 10.10.10.0/24;  
     v6rd-prefix 3040::0/16;  
     mtu-v4 9192;  
   }  
 }  
 rule v6rd-dom1-r1 {  
   match-direction input;  
   term t1 {  
     then {  
       v6rd v6rd-dom1;  
     }  
   }  
 }

### Service Set Configuration

**Step-by-Step Procedure** To configure the service set:

1. Define the service set for 6rd processing.  

```
user@host# top
user@host# edit services service-set v6rd-dom1-service-set
```
2. Define the softwire and stateful firewall rules for the service set.  

```
[edit services service-set v6rd-dom1-service-set]
user@host# set softwire-rules v6rd-dom1
user@host# set stateful-firewall-rules r1
```
3. Define the interface-service for the service set.  

```
[edit services service-set v6rd-dom1-service-set]
user@host# set interface-service service-interface sp-0/2/0
```

**Results** [edit service-set v6rd-dom1-service-set]  
 user@host# show  
 softwire-rules v6rd-dom1-r1  
 interface-service {  
   service-interface sp-0/2/0;  
 }

- Related Documentation**
- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 71](#)
  - [Configuring a 6rd Softwire Concentrator on page 344](#)
  - [Configuring Softwire Rules on page 345](#)
  - [Configuring Stateful Firewall Rules for 6rd Softwire on page 345](#)
  - [Configuring Service Sets for Softwire on page 346](#)
  - [Example: Basic DS-Lite Configuration on page 347](#)
  - [Example: Configuring DS-Lite and 6rd in the Same Service Set on page 358](#)

## Example: Configuring DS-Lite and 6rd in the Same Service Set

---

- [Requirements on page 358](#)
- [Overview on page 358](#)
- [Configuration on page 358](#)

### Requirements

The following hardware components can perform DS-Lite:

- M Series Multiservice Edge routers with Multiservices PICs
- T Series Core routers with Multiservices PICs
- MX Series 3D Universal Edge routers with Multiservices DPCs

### Overview

This example describes a software solution that includes DS-Lite and 6rd in the same service set.

### Configuration

#### Chassis Configuration

---

##### Step-by-Step Procedure

To configure the chassis:

1. Configure the ingress interface.

```
user@host# edit interfaces ge-1/2/0
[edit interfaces ge-1/2/0]
user@host# set unit 0 family inet service input service-set v6rd-dslite-service-set
user@host# set unit 0 family inet service output service-set v6rd-dslite-service-set
user@host# set unit 0 family inet address address 10.10.10.1/24
user@host# set unit 0 family inet6 service input service-set v6rd-dslite-service-set
user@host# set unit 0 family inet6 service output service-set v6rd-dslite-service-set
user@host# set unit 0 family inet6 address address address 2001::1/16
```

Here the service set is applied on the inet (IPv4) and inet6 (IPv6) families of subunit 0. Both DS-Lite IPv6 traffic and 6rd IPv4 traffic hits the service filter and is sent to the services PIC.

2. Configure the egress interface (IPv6 Internet). The IPv4 server that the DS-Lite clients are trying to reach is at 200.200.200.2/24, and the IPv6 server is at 3ABC::2/16.

```
user@host# edit interfaces ge-1/2/2
[edit interfaces ge-1/2/2]
user@host# set unit 0 family inet address 200.200.200.1/24
user@host# set unit 0 family inet6 address 3ABC::1/16
```

3. Configure the services PIC.

```
user@host# edit interfaces sp-3/0/0
[edit interfaces sp-3/0/0]
```

```

user@host# set unit 0 family inet
user@host# set unit 0 family inet6

```

**Results** [edit interfaces]

```

user@host# show
ge-1/2/0 {
  unit 0 {
    family inet {
      service {
        input {
          service-set v6rd-dslite-service-set;
        }
        output {
          service-set v6rd-dslite-service-set;
        }
      }
      address 10.10.10.1/24;
    }
    family inet6 {
      service {
        input {
          service-set v6rd-dslite-service-set;
        }
        output {
          service-set v6rd-dslite-service-set;
        }
      }
      address 2001::1/16;
    }
  }
}
ge-1/2/2 {
  unit 0 {
    family inet {
      address 200.200.200.1/24;
    }
    family inet6 {
      address 3ABC::1/16;
    }
  }
}
sp-3/0/0 {
  unit 0 {
    family inet;
    family inet6;
  }
}

```

### Software Concentrator, Software Rule, Stateful Firewall Rule Configuration

#### Step-by-Step Procedure

To configure the software concentrator, software rule, and stateful firewall rule:

1. Configure the DS-Lite and 6rd software concentrators.

```

user@host# edit services software software-concentrator ds-lite ds1
[edit services software software-concentrator ds-lite ds1]
user@host# set software-address 1001::1
user@host# mtu-v6 9192
usert@host# up 1

```

```

user@host# edit v6rd v6rd-dom1
[edit services software-concentrator v6rd v6rd-dom1]
user@host# set software-address 30.30.30.1
user@host# set ipv4-prefix 10.10.10.0/24
user@host# set v6rd-prefix 3040::0/16
user@host# set mtu-v4 9192

```

2. Configure the software rules.

```

user@host# edit services software rule v6rd-r1]
[edit services software rule v6rd-r1]
user@host# set match-direction input
user@host# set term t1 then v6rd v6rd-dom1
user@host# up 1
user@host# edit services software]
[edit services software]
user@host# edit rule dslite-r1
[edit services software rule dslite-r1]
user@host# set term dslite-t1 then ds-lite ds1

```

The following routes are added by the services PIC daemon on the Routing Engine:

```

user@router# run show route 30.30.30.1
inet.0: 43 destinations, 46 routes (42 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

30.30.30.1/32      *[Static/786432] 00:24:11
                  Service to v6rd-dslite-service-set

[edit]
user@router# run show route 3040::0/16

inet6.0: 23 destinations, 33 routes (23 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

3040::/16         *[Static/786432] 00:24:39
                  Service to v6rd-dslite-service-set

user@router# run show route 1001::1
inet6.0: 33 destinations, 43 routes (33 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1001::1/128      *[Static/1] 1w2d 22:05:41
                  Service to v6rd-dslite-service-set

```

3. Configure a stateful firewall rule.

```

user@host# edit services stateful-firewall rule r1
[edit services stateful-firewall rule r1]
user@host# set match-direction input-output
user@host# set term t1 then accept

[edit services stateful-firewall]
rule r1 {
    match-direction input-output;
    term t1 {
        then {
            accept;
        }
    }
}

```

```

Results [edit services software]
user@host# show
software-concentrator {
    ds-lite ds1 {
        software-address 1001::1;
        mtu-v6 9192;
    }
    v6rd v6rd-dom1 {
        software-address 30.30.30.1;
        ipv4-prefix 10.10.10.0/24;
        v6rd-prefix 3040::0/16;
        mtu-v4 9192;
    }
}
rule v6rd-r1 {
    match-direction input;
    term t1 {
        then {
            v6rd v6rd-dom1;
        }
    }
}
rule dslite-r1 {
    match-direction input;
    term dslite-t1 {
        then {
            ds-lite ds1;
        }
    }
}

[edit services stateful-firewall]
user@host# show
rule r1 {
    match-direction input-output;
    term t1 {
        then {
            accept;
        }
    }
}

```

### NAT Configuration for DS-Lite

**Step-by-Step Procedure** To configure NAT for DS-Lite:

1. Configure a NAT pool for DS-Lite.
 

```

user@host# edit services nat pool dslite-pool
[edit services nat pool dslite-pool]
user@host# set address-range low 33.33.33.1 high 33.33.33.32
user@host# set port automatic
      
```
2. Configure a NAT rule.
 

```

user@host# up 1
[edit services nat rule dslite-nat-r1]
user@host# set match-direction input
      
```

```
user@host# set term dslite-nat-t1 from source-address 20.20.0.0/16 then translated  
translation-type napt-44
```

```

Results [edit services nat]
user@host# show
pool dslite-pool {
    address-range low 33.33.33.1 high 33.33.33.32;
    port {
        automatic;
    }
}
rule dslite-nat-r1 {
    match-direction input;
    term dslite-nat-t1 {
        from {
            source-address {
                20.20.0.0/16;
            }
        }
        then {
            translated {
                source-pool dslite-pool;
                translation-type {
                    source dynamic;
                }
            }
        }
    }
}

```

Because of this NAT rule, the following NAT routes are installed for the reverse DS-Lite traffic:

```

user@router# run show route 33.33.33.0/24
inet.0: 48 destinations, 52 routes (47 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

33.33.33.1/32      *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.2/31      *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.4/30      *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.8/29      *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.16/28     *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.32/32     *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set

```

The NAT rule triggers address translation for the traffic coming from 20.20.0.0/16 to public address range 33.33.33.1 to 33.33.33.32.

### Service Set Configuration

#### Step-by-Step Procedure

This service set has a stateful firewall rule and 6rd rule for 6rd service. The service set also includes a software rule for DS-Lite and a NAT rule to perform address translation for all DS-Lite traffic. The NAT rule performs NATPT translation in the forward direction on the source address and port of the DS-Lite traffic.

To configure the service set:

1. Define the service set.  

```
user@host# edit services service-set v6rd-dslite-service-set
```
2. Configure the service set rules.  

```
[edit services service-set v6rd-dslite-service-set]
user@host# set software-rules dslite-r1
user@host# set stateful-firewall-rules r1
user@host# set nat-rules dslite-nat-r1
```
3. Configure the service set interface-service.  

```
[edit services service-set v6rd-dslite-service-set]
user@host# set interface-service service-interface sp-3/0/0
```

**Results**

```
[edit services service-set]
user@host# show
v6rd-dslite-service-set {
  software-rules v6rd-r1;
  software-rules dslite-r1;
  stateful-firewall-rules r1;
  nat-rules dslite-nat-r1;
  interface-service {
    service-interface sp-3/0/0;
  }
}
```

- Related Documentation**
- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 71](#)
  - [Configuring Service Sets for Software on page 346](#)
  - [Example: Basic DS-Lite Configuration on page 347](#)
  - [Example: Basic 6rd Configuration on page 353](#)

---

## Configuring a 6to4 Provider-Managed Tunnel

When configuring a 6to4 provider-managed tunnel (PMT), replace the Anycast destination with the address of a managed relay in the provider network.

To configure a 6to4 PMT:

1. Configure the ingress interface for 6to4 traffic. Include the name of the service set that identifies the rules for input and output service on this interface.  

```
[edit interfaces ge-0/2/1]
user@host# set unit logical-unit-number family family service input service-set-name
user@host# set unit logical-unit-number family family service output service-set-name
user@host# set unit logical-unit-number family family address address
```

For example:

```
[edit interfaces ge-0/2/1]
user@host# set unit 0 family inet service input service-set v6to4-pmt
user@host# set unit 0 family inet service output service-set v6to4-pmt
user@host# set unit 0 family inet address 130.130.130.1/24
```

2. Configure the egress interface.

```
[edit interfaces ge-0/2/2]
user@host# set unit logical-unit-number family family address address
```

For example:

```
[edit interfaces ge-0/2/2]
user@host# set unit 0 family inet6 address 4ABC::1/16
```

3. Configure the service interface that contains the rules for processing incoming traffic. Include a syslog option and associate a logical unit.

```
[edit interfaces sp-2/0/0]
user@host# edit services-options syslog host host-name services any
user@host# edit unit logical-unit-number family family
user@host# edit unit 0 family family
```

For example:

```
[edit interfaces sp-2/0/0]
user@host# set services-options syslog host local services any
user@host# set unit 0 family inet
user@host# set unit 0 family inet6
```

4. Configure the software concentrator and software rule for 6to4. In the Junos OS, 6to4 PMT configuration uses the same options as 6rd.

```
[edit services software software-concentrator v6rd v6to4]
user@host# set software-address software-address
user@host# set ipv4-prefix ipv4-prefix
user@host# set v6rd-prefix v6rd-prefix
user@host# set mtu-v4 mtu-v4
```

For example:

```
[edit services software software-concentrator v6rd v6to4]
user@host# set software-address 192.88.99.1
user@host# set ipv4-prefix 130.130.130.2/32
user@host# set v6rd-prefix 2002::0/16
user@host# set mtu-v4 9192
```

5. Define the software rule that will process traffic on the ingress interface.

```
[edit services software rule v6to4-r1]
user@host# set match-direction input
user@host# set term term-name then v6rd software-concentrator
```

For example:

```
[edit services software rule v6to4-r1]
user@host# set match-direction input
user@host# set term t1 then v6rd v6to4
```

6. Define a stateful firewall rule that will accept all incoming traffic on the ingress interface.

```
[edit services stateful-firewall rule sfw-r1]
user@host# set match-direction direction
user@host# set term term-name then accept
user@host# set term term-name then syslog
```

For example:

```
[edit services stateful-firewall rule sfw-r1]
user@host# set match-direction input-output
user@host# set term t1 then accept
user@host# set term t1 then syslog
```

7. Define the NAT pool to be used for IPv6 NAT translation. This pool supports translation of the Anycast 6to4 relay addresses to addresses at the provider-managed relay.

```
[edit services nat pool v6to4-pmt]
user@host# set address address
user@host# port automatic
```

For example:

```
[edit services nat pool v6to4-pmt]
user@host# set address 3ABC::1/128
user@host# set port automatic
```

8. Define the NAT rule for translation.

```
[edit services nat rule rule-name]
user@host# set match-direction input
user@host# set term term-name then translated source-pool pool-name
user@host# set term t1 then translated translation-type translation-type
```

For example:

```
[edit services nat rule v6to4-pmt-r1]
user@host# set match-direction input
user@host# set term t1 then translated source-pool v6to4-pmt
user@host# set term t1 then translated translation-type napt-66
```

9. Define the service set that specifies the software rule and NAT rule.

```
[edit services service-set v6to4-pmt]
user@host# set software-rules rule-name
user@host# set stateful-firewall-rules rule-name
user@host# set nat-rules rule-name
user@host# set interface-service service-interface interface-name
```

For example:

```
[edit services service-set v6to4-pmt]
user@host# set software-rules v6to4-r1
user@host# set stateful-firewall-rules sfw-r1
user@host# set nat-rules v6to4-pmt-r1
user@host# set interface-service service-interface sp-2/0/0
```

## CHAPTER 9

# Summary of Software Services Configuration Statements

The following sections explain each of the software services statements. The statements are organized alphabetically.

- [ds-lite on page 368](#)
- [rule \(Software\) on page 369](#)
- [rule-set \(Software\) on page 369](#)
- [software-concentrator on page 370](#)
- [software-rules on page 370](#)
- [v6rd on page 371](#)

## ds-lite

---

Syntax	<pre>ds-lite <i>ds-lite-software-concentrator</i> {     auto-update-mtu;     copy-dscp;     flow-limit <i>flow-limit</i>   session-limit-per-prefix <i>session-limit-per-prefix</i>;     mtu-v6 <i>mtu-v6</i>;     software-address <i>software-address</i>; }</pre>
Hierarchy Level	[edit services software <a href="#">software-concentrator</a> ]
Release Information	<p>Statement introduced in Junos OS Release 10.4.</p> <p><b>auto-update-mtu</b> option introduced in Junos OS Release 10.4.</p> <p><b>copy-dscp</b> option introduced in Junos OS Release 11.2.</p> <p><b>mtu-v6</b> option introduced in Junos OS Release 10.4.</p> <p><b>software-address</b> option introduced in Junos OS Release 10.4.</p>
Description	Configure settings for a DS-Lite concentrator used to process IPv4 packets encapsulated in IPv6.
Options	<p><b><i>ds-lite-software-concentrator</i></b>—Name applied to a DS-Lite software concentrator.</p> <p><b>auto-update-mtu</b>—This option is not currently supported.</p> <p><b>copy-dscp</b>—Copy DSCP information to IPv4 headers during decapsulation.</p> <p><b><i>flow-limit</i></b>—Maximum number of IPv4 flows per software. <b>Range:</b> 0 through 16384 flows</p> <p><b><i>mtu-v6</i></b>—Maximum transmission unit (MTU), in bytes, for encapsulating IPv4 packets into IPv6. If the final length is greater than the configured value, the IPv6 packet is fragmented. <b>Range:</b> 0 through 9192 bytes</p> <p><b><i>session-limit-per-prefix</i></b>—Maximum number of sessions per B4 subnet prefix. (0 through 16384). <b>Range:</b> 0 through 16384 sessions</p> <p><b><i>software-address</i></b>—Address of the DS-Lite software concentrator.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring a DS-Lite Software Concentrator on page 343</a></li></ul>

## rule (Software)

<b>Syntax</b>	<pre>rule rule-name {   match-direction (input   output);   term term-name {     then {       (ds-lite ds-lite-software-concentrator   v6rd v6rd-software-concentrator);     }   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> software], [edit <a href="#">services</a> software rule-set <i>rule-set-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure a rule to apply a software concentrator for a flow.
<b>Options</b>	<p><b>rule-name</b>—Identifier for the collection of terms that constitute this rule.</p> <p><b>input</b>—Apply the rule match on the input side of the interface.</p> <p><b>output</b>—Apply the rule match on the output side of the interface.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Software Rules on page 345</a></li> </ul>

## rule-set (Software)

<b>Syntax</b>	<pre>rule-set rule-set-name {   rule rule-name; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> software]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<b>rule-set-name</b> —Identifier for the collection of rules that constitute this rule set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Software Rules on page 345</a></li> </ul>

## software-concentrator

---

<b>Syntax</b>	<pre>software-concentrator {   ds-lite ds-lite-software-concentrator {     auto-update-mtu;     flow-limit <i>flow-limit</i>   session-limit-per-prefix <i>session-limit-per-prefix</i>;     mtu-v6 <i>mtu-v6</i>;     software-address <i>address</i>;   }   v6rd v6rd-software-concentrator {     ipv4-prefix <i>ipv4-prefix</i>;     v6rd-prefix <i>ipv6-prefix</i>;     mtu-v4 <i>mtu-v4</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit services software]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure settings for a software concentrator.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a DS-Lite Software Concentrator on page 343</a></li><li>• <a href="#">Configuring a 6rd Software Concentrator on page 344</a></li></ul>

## software-rules

---

<b>Syntax</b>	(software-rule <i>rule-name</i>   software-rule-sets <i>rule-set-name</i> );
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">service-set</a> <i>service-set-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the DS-Lite or 6rd rules or rule set included in this service set. You can configure multiple rules; however, you can only configure one rule set for each service set.
<b>Options</b>	<i>rule-name</i> —Identifier for the collection of terms that constitute this rule.  <i>rule-set-name</i> —Identifier for the set of rules to be included.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Rules on page 747</a></li></ul>

## v6rd

<b>Syntax</b>	<pre>v6rd v6rd-softwire-concentrator {   ipv4-prefix <i>ipv4-prefix</i>;   v6rd-prefix <i>ipv6-prefix</i>;   mtu-v4 <i>mtu-v4</i>;   softwire-address <i>ipv4-address</i>; }</pre>
<b>Hierarchy Level</b>	[edit services softwire <a href="#">softwire-concentrator</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure settings for a 6rd concentrator used to process IPv6 packets encapsulated in IPv4 packets.
<b>Options</b>	<p><i>ipv4-prefix</i>—IPv4 prefix of the customer edge (CE) network</p> <p><i>ipv6-prefix</i>—IPv6 prefix of the 6rd domain.</p> <p><i>mtu-v4</i>—Maximum transmission unit (MTU), in bytes (576 through 9192), for IPv6 packets encapsulated into IPv4. If the final length is greater than the configured value, the IPv4 packet will be dropped.</p> <p><i>address</i>—IPv4 address of a softwire concentrator. This is an IPv4 address independent of any interface and on a different prefix.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring a 6rd Softwire Concentrator on page 344</a></li> </ul>



## CHAPTER 10

# Network Address Translation and Software Administration

- [Monitoring Carrier-Grade NAT and Software on page 373](#)
- [Ping and Traceroute for DS-Lite on page 377](#)
- [Log Generation on page 377](#)
- [Configuring NAT Session Logs on page 378](#)
- [High Availability and Load Balancing for 6rd Softwires on page 379](#)
- [Protecting Against Denial of Service Attacks on page 384](#)

## Monitoring Carrier-Grade NAT and Software

---

### Monitoring CGN, Stateful Firewall, and Software Flows

**Purpose** Use the following commands to check the creation of the softwires, pre-NAT flows, and post-NAT flows. Output can be filtered using more specific fields such as AFTR or B4 address or both for DS-Lite, and software-concentrator or software-initiator or both for 6rd.

- *show services stateful-firewall flows*
- *show services software flows*

**Action** user@host# **show services stateful-firewall flows**

Interface: sp-0/1/0, Service set: dslite-svc-set2

Flow	State	Dir	Frm count
TCP 200.200.200.2:80 -> 44.44.44.1:1025	Forward	O	219942
NAT dest 44.44.44.1:1025 -> 20.20.1.4:1025			
Software 2001::2 -> 1001::1			
TCP 20.20.1.2:1025 -> 200.200.200.2:80	Forward	I	110244
NAT source 20.20.1.2:1025 -> 44.44.44.1:1024			
Software 2001::2 -> 1001::1			
TCP 200.200.200.2:80 -> 44.44.44.1:1024	Forward	O	219140
NAT dest 44.44.44.1:1024 -> 20.20.1.2:1025			
Software 2001::2 -> 1001::1			
DS-LITE 2001::2 -> 1001::1	Forward	I	988729
TCP 200.200.200.2:80 -> 44.44.44.1:1026	Forward	O	218906
NAT dest 44.44.44.1:1026 -> 20.20.1.3:1025			
Software 2001::2 -> 1001::1			
TCP 20.20.1.3:1025 -> 200.200.200.2:80	Forward	I	110303
NAT source 20.20.1.3:1025 -> 44.44.44.1:1026			
Software 2001::2 -> 1001::1			
TCP 20.20.1.4:1025 -> 200.200.200.2:80	Forward	I	110944
NAT source 20.20.1.4:1025 -> 44.44.44.1:1025			
Software 2001::2 -> 1001::1			

- Related Documentation**
- *NAT Objects MIB in SNMP MIBs and Traps Reference*
  - *Network Address Translation Resources—Monitoring MIB in SNMP MIBs and Traps Reference*
  - *Juniper Networks Enterprise-Specific NAT Traps on SRX Series Services Gateways in SNMP MIBs and Traps Reference*

## Monitoring Stateful Firewall Conversations

**Purpose** Use the **show services stateful-firewall conversations** command to show conversations, or collections of related flows.

**Action** user@host# **show services stateful-firewall conversations**

Interface: sp-0/0/0, Service set: sset

Conversation: ALG protocol: tcp

Number of initiators: 1, Number of responders: 1

Flow State Dir Frm

count

TCP 10.0.0.1:1025 -> 128.0.0.1:80 Forward I 372755

NAT source 10.0.0.1:1025 -> 129.0.0.1:1024

Software 2001:0:0:1::1 -> 1001::1

TCP 128.0.0.1:80 -> 129.0.0.1:1024 Forward O 794083

NAT dest 129.0.0.1:1024 -> 10.0.0.1:1025

Software 2001:0:0:1::1 -> 1001::1

## Monitoring Global Stateful Firewall Statistics

**Purpose** Use the **show services stateful-firewall statistics** command to observe statistics for service sets containing software rules.

**Action** user@host# **show services stateful-firewall statistics**  
 Interface Service set Accept Discard Reject Errors  
 sp-0/0/0 dslite-svc-set2 118991296 0 0 0  
 sp-0/1/0 dslite-svc-set1 237615050 0 0 0

## Monitoring NAT Pool Usage

**Purpose** Use the **show services nat pool detail** command to find global NAT statistics related to pool usage. This command is frequently used in conjunction with the **show services stateful-firewall statistics** command.

**Action** user@host# **show services nat pool detail**

```
Interface: ms-1/0/0, Service set: s1
  NAT pool: dest-pool, Translation type: DNAT-44
    Address range: 10.10.10.2-10.10.10.2
  NAT pool: napt-pool, Translation type: NAPT-44
    Address range: 50.50.50.1-50.50.50.254
    Port range: 1024-63487, Ports in use: 0, Out of port errors: 0, Max ports
used: 0
  NAT pool: source-dynamic-pool, Translation type: DYNAMIC NAT44
    Address range: 40.40.40.1-40.40.40.254
    Out of address errors: 0, Addresses in use: 0
  NAT pool: source-static-pool, Translation type: BASIC NAT44
    Address range: 30.30.30.1-30.30.30.254
```

- Related Documentation**
- *NAT Objects MIB in SNMP MIBs and Traps Reference*
  - *Network Address Translation Resources—Monitoring MIB in SNMP MIBs and Traps Reference*
  - *Juniper Networks Enterprise-Specific NAT Traps on SRX Series Services Gateways in SNMP MIBs and Traps Reference*

## Monitoring Software Statistics

**Purpose** You can review software global statistics by using the **show services software** or **show services software statistics** command.

```
Action user@host# show services software
Interface: sp-0/0/0, Service set: sset
Software Direction Flow count
2001:0:0:1::1 -> 1001::1 I 3

user@host# show services software statistics
DS-Lite Statistics:
Service PIC Name: :sp-0/0/0
Statistics
-----
Softwires Created :2
Softwires Deleted :1
Softwires Flows Created :2
Softwires Flows Deleted :1
Slow Path Packets Processed :2
Fast Path Packets Processed :274240
Fast Path Packets Encapsulated :583337
Rule Match Failed :0
Rule Match Succeeded :2
IPv6 Packets Fragmented :0
Transient Errors
-----
Flow Creation Failed - Retry :0
Slow Path Failed - Retry :0
Errors
-----
Software Creation Failed :0
Flow Creation Failed :0
Slow Path Failed :0
Packet not IPv4-in-IPv6 :0
IPv6 Fragmentation Error :0
Slow Path Failed - IPv6 Next Header Offset :0
Decapsulated Packet not IPv4 :0
Fast Path Failed - IPv6 Next Header Offset :0
No Software ID :0
No Flow Extension :0
Flow Limit Exceeded :0
6rd Statistics:
Service PIC Name :sp-0/0/0
Statistics
-----
Softwires Created :0
Softwires Deleted :0
Softwires Flows Created :0
Softwires Flows Deleted :0
Slow Path Packets Processed :0
Fast Path Packets Processed :0
Fast Path Packets Encapsulated :0
Rule Match Failed :0
Rule Match Succeeded :0
Transient Errors
-----
Flow Creation Failed - Retry :0
Slow Path Failed - Retry :0
Errors
-----
Software Creation Failed :0
Flow Creation Failed :0
Slow Path Failed :0
Packet not IPv6-in-IPv4 :0
```

```

Slow Path Failed - IPv6 Next Header Offset :0
Decapsulated Packet not IPv6 :0
Encapsulation Failed - No packet memory :0
No Software ID :0
No Flow Extension :0
ICMPv4 Dropped Packets :0

```

## Ping and Traceroute for DS-Lite

With Junos OS Release 11.4, you can use the **ping** and **traceroute** commands to determine the status of the DS-Lite software tunnels:

- **IPv6 ping**—The software address endpoint on the DS-Lite software terminator (AFTR) is usually configured only at the **[edit services software]** hierarchy level; it need not be hosted on any interface. Previous releases of the Junos OS software did not provide replies to pings to the IPv6 software address when the AFTR was not configured on a specific interface or loopback. An IPv6 ping enables the software initiator (B4) to verify the software address of the AFTR before creating a tunnel.
- **IPv4 ping**—A special IPv4 address, 192.0.0.1, is reserved for the AFTR. Previous releases of the Junos OS did not respond to any pings sent to this address. A B4 and other IPv4 nodes can now ping to this address to determine whether the DS-Lite tunnel is working.
- **Traceroute**—The AFTR now generates and forwards traceroute packets over the DS-Lite tunnel.



**NOTE:** No additional CLI configuration is necessary to use the new functionality.

## Log Generation

The Multiservices PIC uses the system logging protocol to generate session logging. System log messages can be sent directly from the services PIC to an external system logging server. This requires that the services PIC interface have an IP address and appropriate system logging options configured, as in this example:

```

[edit interfaces sp-5/0/0]
services-options {
  syslog {
    host 130.0.0.1 {
      services any;
    }
  }
}
unit 0 {
  family inet {
    address 150.0.0.1/32;
  }
}

```

## Log Format

For each session, three logs are generated. The three logs allow correlation of start and end times for each session.

```
Jun 28 15:29:20 cypher (FPC Slot 5, PIC Slot 0) {sset2}[FWNAT]:
ASP_SFW_CREATE_ACCEPT_FLOW: proto 6 (TCP) application: any,
ge-1/3/5.0:10.0.0.1:8856 -> 128.0.0.2:80, creating forward or watch flow ; source
address and port translate to 129.0.0.1:1028
Jun 28 15:29:23 cypher (FPC Slot 5, PIC Slot 0)
{sset2}[FWNAT]:ASP_NAT_POOL_RELEASE: natpool release 129.0.0.1:1028[1]
Jun 28 15:29:23 cypher (FPC Slot 5, PIC Slot 0) {sset2}[FWNAT]:
ASP_SFW_DELETE_FLOW: proto 6 (TCP) application: any, (null)(null)10.0.0.1:8856
-> 128.0.0.2:80, deleting forward or watch flow ; source address and port translate
to 129.0.0.1:1028
```

Log format varies somewhat depending on interface card. The example show is for the MS-DPC.

## System Log Throttling

You can limit logging with the [message-rate-limit](#) command.



**NOTE:** in next-hop based service sets, the log sent to remote syslog server comes to the packet forwarding engine (PFE) via the output services PIC interface. This means that you must configure routing properly in the routing-instance where the output interface is configured.

- Related Documentation**
- [message-rate-limit on page 776](#)
  - [Configuring System Logging for Service Sets on page 754](#)

---

## Configuring NAT Session Logs

You can configure session logs for NAT from the CLI. By default, session open and close logs are produced. However, you can request that only one type of log be produced.

To configure NAT session logs:

1. Go to the `[edit services service-set service-set-name syslog host class classname]` hierarchy level.  

```
user@host# edit services service-set service-set-name syslog host class classname
```
2. Configure NAT logging using the **nat-logs** configuration statement.  

```
[edit services service-set service-set-name syslog host class classname]
user@host# set nat-logs.
```
3. Configure session logging using the **session-logs** statement. Open and close logs are produced by default. Specify **open** or **close** to produce only one type of log.  

```
[edit services service-set service-set-name syslog host class classname]
user@host# set session-logs.
```

Or

```
[edit services service-set service-set-name syslog host class classname]
user@host# set session-logs open.
```

Or

```
[edit services service-set service-set-name syslog host class classname]
user@host# set session-logs close.
```

4. For NAT sessions that use secured port block allocation (PBA), enter the **pba-interim-logging interval** option.

```
[edit services service-set service-set-name syslog host class classname]
user@host# top.
[edit]
user@host# set interfaces interface-name service-options
    pba-interim-logging-interval.
```

#### Related Documentation

- [Configuring System Logging for Service Sets on page 754](#)
- [Interim Logging for Port Block Allocation on page 199](#)

## High Availability and Load Balancing for 6rd Softwires

- [Load Balancing a 6rd Domain Across Multiple Services PICs on page 379](#)
- [Example: Load Balancing a 6rd Domain Across Multiple Services PICs on page 379](#)
- [Configuring High Availability for 6rd Using 6rd Anycast on page 384](#)

### Load Balancing a 6rd Domain Across Multiple Services PICs

The 6rd domain is an IPv6 network, which can potentially be very large. A single PIC, or network processing unit (NPU) on a Multiservices DPC, might not be able to handle all the traffic for the 6rd domain. To alleviate load problems, you can load-balance the 6rd domain traffic across multiple PICs. To do so, assign the same software rule to different services sets that use different interfaces. Configure explicit routes and equal-cost multipath (ECMP) to load-balance the 6rd traffic.

#### Example: Load Balancing a 6rd Domain Across Multiple Services PICs

- [Hardware and Software Requirements on page 379](#)
- [Overview on page 380](#)
- [Configuration on page 380](#)

#### Hardware and Software Requirements

This example requires the following hardware:

- An MX Series 3D Universal Edge router with a services DPC with two available NPUs or an M Series Multiservice Edge router with two services PICs available for 6rd software concentrator processing
- A domain name server (DNS)

This example uses the following software:

- Junos OS Release 11.4 or higher

---

## Overview

Because of anticipated volume, a provider needs to balance 6rd software traffic between two services PICs.

---

## Configuration

- [Chassis Configuration on page 380](#)
- [Software Concentrator and Software Rule Configuration on page 381](#)
- [Stateful Firewall Configuration on page 381](#)
- [Service Set Configuration on page 382](#)
- [Load-Balancing Configuration on page 382](#)

### *Chassis Configuration*

#### **Step-by-Step Procedure**

To configure the chassis:

1. Define the ingress interface and its properties.  

```
user@host# edit interfaces ge-1/2/0
user@host# set unit 0 family inet address 10.10.10.1/16
```
2. Define the egress interface and its properties. In this example, the IPv6 clients try to reach the IPv6 server at 3abc::2/16.  

```
user@host# edit interfaces ge-1/2/2
user@host# set unit 0 family inet6 address 3ABC::1/16
```
3. Define the services PICs for selection as software concentrators by the load-balancing process. This configuration uses two PICs/NPUs: sp-3/0/0 and sp-3/1/0. A next-hop style service set is configured (shown in the next section).  

```
user@host# edit interfaces sp-3/0/0
[edit interfaces ge-3/0/0]
user@host# set services-options syslog host local services any
user@host# set unit 0 family inet
user@host# set unit 0 family inet6
user@host# set unit 1 family inet service-domain inside
user@host# set unit 1 family inet service-domain outside
user@host# set unit 2 family inet service-domain inside
user@host# set unit 2 family inet service-domain outside
user@host# up 1
[edit]
user@host# edit interfaces sp-3/1/0
[edit interfaces sp-3/1/0]
user@host# set services-options syslog host local services any
user@host# set unit 0 family inet
user@host# set unit 0 family inet6
user@host# set unit 1 family inet service-domain inside
user@host# set unit 1 family inet service-domain outside
user@host# set unit 2 family inet service-domain inside
user@host# set unit 2 family inet service-domain outside
```

**Software Concentrator and Software Rule Configuration**

**Step-by-Step Procedure** The software configuration is straightforward. In this example, the 6rd domain prefix is 3040::0/16, the 6rd software concentrator IPv4 address is 30.30.30.1, and the customer IPv4 network is 10.10.0.0/16. In the customer premises equipment (CPE) network, all customer edge (CE) devices have addresses that belong to the 10.10.0.0/16 network. To configure the software:

1. Go to the **[edit services software]** hierarchy level.  

```
user@host# edit services software
```
2. Configure IPv6 multicast.  

```
[edit services software]
user@host# set ipv6-multicast-interfaces all
```
3. Go to the software concentrator v6rd hierarchy level and name the software concentrator **shenick01-rd1**.  

```
[edit services software]
user@host# edit software-concentrator v6rd shenick01-rd1
```
4. Configure the software concentrator properties.  

```
[edit services software software-concentrator v6rdshenick01-rd1 ]
user@host# set software-address 30.30.30.1
user@host# set ipv4-prefix 10.10.0.0/16
user@host# set v6rd-prefix 3040::/16
user@host# set mtu-v4 9192
```
5. Configure a software rule for incoming 6rd traffic.  

```
[edit services software software-concentrator v6rd shenick01-rd1 ]
user@host# up 1
[edit services software ]
user@host# edit rule shenick01-r1
[edit services software rule shenick01-r1]
user@host# set match-direction input
user@host# set term t1 then v6rd shenick01-rd1
```

**Stateful Firewall Configuration**

**Step-by-Step Procedure** To configure the stateful firewall rule:

1. Go to the stateful firewall hierarchy level and define a rule.  

```
user@host# edit services stateful-firewall rule r1
```
2. Set the match direction.  

```
[edit services stateful-firewall rule r1]
user@host# set match-direction input-output
```
3. Configure a term that accepts all traffic.  

```
[edit services stateful-firewall rule r1]
user@host# set term t1 then accept
```

### *Service Set Configuration*

**Step-by-Step Procedure** This configuration provides two service sets, each pointing to a different network processing unit (NPU). Both service sets use the same stateful firewall and software rules. Because they use the same software rule, they refer to same 6rd software concentrator. This results in the software concentrator being hosted on both the NPUs.

To configure the service set:

1. Define a service set for the first NPU.  

```
user@host# edit services service-set v6rd-sset1
```
2. Configure the software and stateful firewall rules for the first NPU.  

```
[edit services service-set v6rd-sset1]  
user@host# set software-rules shenick01-r1  
user@host# set stateful-firewall-rules r1
```
3. Configure the inside and outside interfaces for the next-hop service.  

```
[edit services service-set v6rd-sset1]  
user@host# set next-hop-service inside-service-interface sp-3/0/0.1  
user@host# set next-hop-service outside-service-interface sp-3/0/0.2
```
4. Define a service set for the second NPU.  

```
user@host# edit services service-set v6rd-sset2
```
5. Configure the software and stateful firewall rules for the second NPU.  

```
[edit services service-set v6rd-sset2]  
user@host# set software-rules shenick01-r1  
user@host# set stateful-firewall-rules r1
```
6. Configure the inside and outside interfaces for the next-hop service.  

```
[edit services service-set v6rd-sset1]  
user@host# set next-hop-service inside-service-interface sp-3/1/0.1  
user@host# set next-hop-service outside-service-interface sp-3/1/0.2
```

### *Load-Balancing Configuration*

**Step-by-Step Procedure** To configure load balancing:  
Configure explicit routes and ECMP to load-balance the 6rd traffic. Configure explicit routes for both the 6rd concentrator IPv4 address and the 6rd domain prefix, so that they point to both NPUs.

1. To configure static routes for the 6rd domain using the routing-table inet6.0, go to the **[edit forwarding-options rib inet6.0 static]** hierarchy level and set the routes for the 6rd domain and the 6rd concentrator IPv4 address.  

```
user@host edit forwarding-options rib inet6.0 static  
[edit forwarding-options rib inet6.0 static]  
user@host# set route 3040::0/16 next-hop [ sp-3/0/0.2 sp-3/1/0.2 ]  
user@host# set route 30.30.30.1/32 next-hop [ sp-3/0/0.1 sp-3/1/0.1 ]
```

The service PIC daemon (spd) also adds default routes to these addresses pointing to the NPUs. However, the routes added by the spd use different metrics, which are computed based on the FPC, PIC, slot numbers, and subunit of the services PIC if used in the service set configuration. The static routes configured in this sample configuration will have metrics of 5 and therefore a higher preference than the spd-added routes.

The explicitly configured routes are as follows:

```
root@router# run show route 30.30.30.1
inet.0: 37 destinations, 40 routes (36 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

30.30.30.1/32      *[Static/5] 00:00:10
                  > via sp-3/0/0.1
                  via sp-3/1/0.1
                  [Static/786433] 00:23:03
                  > via sp-3/0/0.1
                  [Static/851969] 00:00:09
                  > via sp-3/1/0.1

root@router# run show route 3040::/16
inet6.0: 20 destinations, 33 routes (20 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

3040::/16         *[Static/5] 00:00:15
                  via sp-3/0/0.2
                  > via sp-3/1/0.2
                  [Static/786434] 00:23:08
                  > via sp-3/0/0.2
                  [Static/851970] 00:00:14
                  > via sp-3/1/0.2
```



**BEST PRACTICE:** The spd-installed routes have higher metric values (hence a low preference) and the metrics are different. If the metrics are different and ECMP is not enabled, even though multiple routes exist for the same destination, only one of the routes is picked up all the time (based on the metric). For ECMP you must configure equal-cost routes, and hence a manual configuration of routes is needed as shown above.

2. Configure equal-cost multipath (ECMP) load balancing by configuring the hash key at the **[edit forwarding-options hash-key]** hierarchy level.

```
user@host# forwarding-options hash-key
[edit forwarding-options hash-key]
user@host# set family inet layer-3 destination-address
user@host# set family inet layer-3 source-address
user@host# set family inet6 layer-3 destination-address
user@host# set family inet6 layer-3 source-address
```

3. Verify your configuration by displaying **forwarding-options**.

```
user@host# show forwarding-options
hash-key {
    family inet { <== IPv4 traffic from CEs uses this
```

```
        layer-3 {  
            destination-address;  
            source-address;  
        }  
    }  
    family inet6 { <== IPv6 traffic from Internet uses this  
        layer-3 {  
            destination-address;  
            source-address;  
        }  
    }  
}
```



**TIP:** Both IPv4 and IPv6 hash keys must be configured. The IPv4 hash key is used to distribute the traffic coming from CPE devices to the 6rd branch relay. The IPv6 hash key is used to distribute the traffic coming from the IPv6 Internet to the 6rd domain. Because the hash in the forward and reverse direction is for different families, different flows from the same session can reside on different NPUs. However, 6rd processing is stateless (as far as mapping IPv6 packets to softwires is concerned), so this should not be a problem.

---

## Configuring High Availability for 6rd Using 6rd Anycast

You configure 6rd Anycast by defining two service sets that use the same softwire rule in both service sets, just as you do when you configure load balancing for 6rd. However, you do not configure ECMP, and as a result, the services PIC daemon (spd) installs two routes *each* for the softwire concentrator address and 6rd domain pointing to each service interface. The forwarding plane can select any route based on the priority, which is computed when the spd installs the routes. The priority is computed based on the FPC, PIC, slot numbers, and subunit number used on the sp- interface. *Only one PIC is used* based on the route priority, and that PIC gets all of the 6rd traffic. If the PIC goes down, the route pointing to it is also deleted and the forwarding plane automatically selects the alternate available PIC.

6rd Anycast is completely stateless. The spd installs the route and doesn't run any state machine for the PIC. Because the routes are pre-installed and service sets are already on the PIC, there is no service delay if a failover occurs.

### Related Documentation

- [Junos Address Aware Carrier Grade NAT and IPv6 Feature Guide](#)

---

## Protecting Against Denial of Service Attacks

- [Protecting CGN Devices Against Denial of Service \(DOS\) Attacks on page 385](#)

## Protecting CGN Devices Against Denial of Service (DOS) Attacks

You can now choose configuration options that help prevent or minimize the effect of attempted denial of service (DOS) attacks.

- [Mapping Refresh Behavior on page 385](#)
- [EIF Inbound Flow Limit on page 385](#)

---

### Mapping Refresh Behavior

Prior to the implementation of the new options for configuring NAT mapping refresh behavior, described in this topic, a conversation was kept alive when either inbound or outbound flows were active. This remains the default behavior. You can now also specify mapping refresh for only inbound flows or only outbound flows. To configure mapping refresh behavior, include the **mapping-refresh (inbound | outbound | inbound-outbound)** statement at the **[edit services nat rule *rule-name* term *term-name* then translated secure-nat-mapping]** hierarchy level.

---

### EIF Inbound Flow Limit

Previously, the number of inbound connections on an EIF mapping was limited only by the maximum flows allowed on the system. You can now configure the number of inbound flows allowed for an EIF. To limit the number of inbound connections on an EIF mapping, include the **eif-flow-limit *number-of-flows*** statement at the **[edit services nat rule *rule-name* term *term-name* then translated secure-nat-mapping]** hierarchy level.



# Stateful Firewall Services Configuration Guidelines

To configure stateful firewall services, include the **stateful-firewall** statement at the **[edit services]** hierarchy level:

```
[edit services]
stateful-firewall {
  rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
      from {
        application-sets set-name;
        applications [ application-names ];
        destination-address (address | any-unicast) <except>;
        destination-address-range low minimum-value high maximum-value <except>;
        destination-prefix-list list-name <except>;
        source-address (address | any-unicast) <except>;
        source-address-range low minimum-value high maximum-value <except>;
        source-prefix-list list-name <except>;
      }
      then {
        (accept | discard | reject);
        allow-ip-options [ values ];
        syslog;
      }
    }
  }
  rule-set rule-set-name {
    [ rule rule-names ];
  }
}
```

This chapter contains the following sections:

- [Configuring Stateful Firewall Rules on page 388](#)
- [Configuring Stateful Firewall Rule Sets on page 392](#)
- [Examples: Configuring Stateful Firewall Rules on page 392](#)

## Configuring Stateful Firewall Rules

To configure a stateful firewall rule, include the **rule** *rule-name* statement at the **[edit services stateful-firewall]** hierarchy level:

```
[edit services stateful-firewall]
rule rule-name {
  match-direction (input | output | input-output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address address <except>;
      destination-address-range low minimum-value high maximum-value <except>;
      destination-prefix-list list-name <except>;
      source-address address <except>;
      source-address-range low minimum-value high maximum-value <except>;
      source-prefix-list list-name <except>;
    }
    then {
      (accept | discard | reject);
      allow-ip-options [ values ];
      syslog;
    }
  }
}
```

Each stateful firewall rule consists of a set of terms, similar to a filter configured at the **[edit firewall]** hierarchy level. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded. The **from** statement is optional in stateful firewall rules.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software. The **then** statement is mandatory in stateful firewall rules.

The following sections explain how to configure the components of stateful firewall rules:

- [Configuring Match Direction for Stateful Firewall Rules on page 388](#)
- [Configuring Match Conditions in Stateful Firewall Rules on page 389](#)
- [Configuring Actions in Stateful Firewall Rules on page 390](#)

### Configuring Match Direction for Stateful Firewall Rules

Each rule must include a **match-direction** statement that specifies the direction in which the rule match is applied. To configure where the match is applied, include the **match-direction** statement at the **[edit services stateful-firewall rule rule-name]** hierarchy level:

```
[edit services stateful-firewall rule rule-name]
match-direction (input | output | input-output);
```

If you configure **match-direction input-output**, sessions initiated from both directions might match this rule.

The match direction is used with respect to the traffic flow through the AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.

With a next-hop service set, packet direction is determined by the interface used to route the packet to the AS or Multiservices PIC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the PIC, the packet direction is output. For more information on inside and outside interfaces, see [“Configuring Service Sets to be Applied to Services Interfaces” on page 742](#).

On the PIC, a flow lookup is performed. If no flow is found, rule processing is performed. Rules in this service set are considered in sequence until a match is found. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that matches the packet direction are considered. Most packets result in the creation of bidirectional flows.

## Configuring Match Conditions in Stateful Firewall Rules

To configure stateful firewall match conditions, include the **from** statement at the **[edit services stateful-firewall rule rule-name term term-name]** hierarchy level:

```
[edit services stateful-firewall rule rule-name term term-name]
from {
  application-sets set-name;
  applications [ application-names ];
  destination-address (address | any-unicast) <except>;
  destination-address-range low minimum-value high maximum-value <except>;
  destination-prefix-list list-name <except>;
  source-address (address | any-unicast) <except>;
  source-address-range low minimum-value high maximum-value <except>;
  source-prefix-list list-name <except>;
}
```

The source address and destination address can be either IPv4 or IPv6. You can use either the source address or the destination address as a match condition, in the same way that you would configure a firewall filter; for more information, see the *Routing Policy Feature Guide for Routing Devices*. You can use the wildcard value **any-unicast**, which denotes matching all unicast addresses.

Alternatively, you can specify a list of source or destination prefixes by configuring the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either the **destination-prefix-list** or the **source-prefix-list** statement in the stateful firewall rule. For an example, see [“Examples: Configuring Stateful Firewall Rules” on page 392](#).

If you omit the **from** term, the stateful firewall accepts all traffic and the default protocol handlers take effect:

- User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP) create a bidirectional flow with a predicted reverse flow.
- IP creates a unidirectional flow.

You can also include application protocol definitions you have configured at the **[edit applications]** hierarchy level; for more information, see [“Configuring Application Protocol Properties” on page 146](#).

- To apply one or more specific application protocol definitions, include the **applications** statement at the **[edit services stateful-firewall rule rule-name term term-name from]** hierarchy level.
- To apply one or more sets of application protocol definitions you have defined, include the **application-sets** statement at the **[edit services stateful-firewall rule rule-name term term-name from]** hierarchy level.



**NOTE:** If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the **[edit applications]** hierarchy level; you cannot specify these properties as match conditions.

## Configuring Actions in Stateful Firewall Rules

To configure stateful firewall actions, include the **then** statement at the **[edit services stateful-firewall rule rule-name term term-name]** hierarchy level:

```
[edit services stateful-firewall rule rule-name term term-name]
then {
  (accept | discard | reject);
  allow-ip-options [ values ];
  syslog;
}
```

You must include one of the following three possible actions:

- **accept**—The packet is accepted and sent on to its destination.
- **discard**—The packet is not accepted and is not processed further.
- **reject**—The packet is not accepted and a rejection message is returned; UDP sends an ICMP unreachable code and TCP sends RST. Rejected packets can be logged or sampled.

You can optionally configure the firewall to record information in the system logging facility by including the **syslog** statement at the **[edit services stateful-firewall rule rule-name term term-name then]** hierarchy level. This statement overrides any **syslog** setting included in the service set or interface default configuration.

## Configuring IP Option Handling

You can optionally configure the firewall to inspect IP header information by including the **allow-ip-options** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* then]** hierarchy level. When you configure this statement, all packets that match the criteria specified in the **from** statement are subjected to additional matching criteria. A packet is accepted only when all of its IP option types are configured as values in the **allow-ip-options** statement. If you do not configure **allow-ip-options**, only packets without IP header options are accepted.

The additional IP header option inspection applies only to the **accept** and **reject** stateful firewall actions. This configuration has no effect on the **discard** action. When the IP header inspection fails, reject frames are not sent; in this case, the **reject** action has the same effect as **discard**.

If an IP option packet is accepted by the stateful firewall, Network Address Translation (NAT) and intrusion detection service (IDS) are applied in the same way as to packets without IP option headers. The IP option configuration appears only in the stateful firewall rules; NAT applies to packets with or without IP options.

When a packet is dropped because it fails the IP option inspection, this exception event generates both IDS event and system log messages. The event type depends on the first IP option field rejected.

Table 26 on page 391 lists the possible values for the **allow-ip-options** statement. You can include a range or set of numeric values, or one or more of the predefined IP option settings. You can enter either the option name or its numeric equivalent. For more information, refer to <http://www.iana.org/assignments/ip-parameters>.

**Table 26: IP Option Values**

IP Option Name	Numeric Value	Comment
<b>any</b>	<b>0</b>	Any IP option
<b>ip-security</b>	<b>130</b>	—
<b>ip-stream</b>	<b>136</b>	—
<b>loose-source-route</b>	<b>131</b>	—
<b>route-record</b>	<b>7</b>	—
<b>router-alert</b>	<b>148</b>	—
<b>strict-source-route</b>	<b>137</b>	—
<b>timestamp</b>	<b>68</b>	—

## Configuring Stateful Firewall Rule Sets

---

The **rule-set** statement defines a collection of stateful firewall rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the **rule-set** statement at the **[edit services stateful-firewall]** hierarchy level with a **rule** statement for each rule:

```
[edit services stateful-firewall]
rule-set rule-set-name {
  rule rule-name;
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing continues to the next rule in the rule set. If none of the rules matches the packet, the packet is dropped by default.

## Examples: Configuring Stateful Firewall Rules

---

The following example show a stateful firewall configuration containing two rules, one for input matching on a specified application set and the other for output matching on a specified source address:

```
[edit services]
stateful-firewall {
  rule Rule1 {
    match-direction input;
    term 1 {
      from {
        application-sets Applications;
      }
      then {
        accept;
      }
    }
    term accept {
      then {
        accept;
      }
    }
  }
  rule Rule2 {
    match-direction output;
    term Local {
      from {
        source-address {
          10.1.3.2/32;
        }
      }
      then {
        accept;
      }
    }
  }
}
```

```

    }
  }
}

```

The following example has a single rule with two terms. The first term rejects all traffic in **my-application-group** that originates from the specified source address, and provides a detailed system log record of the rejected packets. The second term accepts Hypertext Transfer Protocol (HTTP) traffic from anyone to the specified destination address.

```

[edit services stateful-firewall]
rule my-firewall-rule {
  match-direction input-output;
  term term1 {
    from {
      source-address 10.1.3.2/32;
      application-sets my-application-group;
    }
    then {
      reject;
      syslog;
    }
  }
  term term2 {
    from {
      destination-address 10.2.3.2/32;
      applications http;
    }
    then {
      accept;
    }
  }
}

```

The following example shows use of source and destination prefix lists. This requires two separate configuration items.

You configure the prefix list at the **[edit policy-options]** hierarchy level:

```

[edit]
policy-options {
  prefix-list p1 {
    1.1.1.1/32;
    2.2.2.0/24;
  }
  prefix-list p2 {
    3.3.3.3/32;
    4.4.4.0/24;
  }
}

```

You reference the configured prefix list in the stateful firewall rule:

```

[edit]
services {
  stateful-firewall {
    rule r1 {

```

```

match-direction input;
term t1 {
  from {
    source-prefix-list {
      p1;
    }
    destination-prefix-list {
      p2;
    }
  }
  then {
    accept;
  }
}
}
}

```

This is equivalent to the following configuration:

```

[edit]
services {
  stateful-firewall {
    rule r1 {
      match-direction input;
      term t1 {
        from {
          source-address {
            1.1.1.1/32;
            2.2.2.0/24;
          }
          destination-address {
            3.3.3.3/32;
            4.4.4.0/24;
          }
        }
        then {
          accept;
        }
      }
    }
  }
}

```

You can use the **except** qualifier with the prefix lists, as in the following example. In this case, the **except** qualifier applies to all prefixes included in prefix list **p2**.

```

[edit]
services {
  stateful-firewall {
    rule r1 {
      match-direction input;
      term t1 {
        from {
          source-prefix-list {
            p1;

```

```
    }  
    destination-prefix-list {  
        p2 except;  
    }  
}  
then {  
    accept;  
}  
}  
}  
}
```

For additional examples that combine stateful firewall configuration with other services and with virtual private network (VPN) routing and forwarding (VRF) tables, see the configuration examples.

**Related  
Documentation**

- [Example: BOOTP and Broadcast Addresses on page 123](#)
- [Example: Dynamic Source NAT as a Next-Hop Service on page 122](#)
- [Example: Virtual Routing and Forwarding \(VRF\) and Service Configuration on page 121](#)
- [Example: Service Interfaces Configuration on page 118](#)
- [Example: Configuring Layer 3 Services and the Services SDK on Two PICs](#)



## CHAPTER 12

# Summary of Stateful Firewall Configuration Statements

The following sections explain each of the stateful firewall services statements. The statements are organized alphabetically.

## allow-ip-options

- Syntax** `allow-ip-options [ values ];`
- Hierarchy Level** `[edit services \(stateful-firewall\) stateful-firewall rule rule-name term term-name then]`
- Release Information** Statement introduced before Junos OS Release 7.4.
- Description** Configure how the stateful firewall handles IP header information. This statement is optional.
- Options** *value*—Can be a set or range of numeric values, or one or more of the following predefined option types. You can enter either the option name or its numeric equivalent.

Option Name	Numeric Value
any	0
ip-security	130
ip-stream	8
loose-source-route	3
route-record	7
router-alert	148
strict-source-route	9
timestamp	4

- Usage Guidelines** See [“Configuring Actions in Stateful Firewall Rules”](#) on page 390.
- Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

## application-sets

---

<b>Syntax</b>	<code>applications-sets <i>set-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services (stateful-firewall)</a> stateful-firewall <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define one or more target application sets.
<b>Options</b>	<i>set-name</i> —Name of the target application set.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Match Conditions in Stateful Firewall Rules</a> ” on page 389.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## applications

---

<b>Syntax</b>	<code>applications [ <i>application-names</i> ];</code>
<b>Hierarchy Level</b>	[edit <a href="#">services (stateful-firewall)</a> stateful-firewall <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define one or more applications to which the stateful firewall services apply.
<b>Options</b>	<i>application-name</i> —Name of the target application.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Match Conditions in Stateful Firewall Rules</a> ” on page 389.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## destination-address

---

Syntax	destination-address ( <i>address</i>   any-unicast) <except>;
Hierarchy Level	[edit <a href="#">services (stateful-firewall)</a> stateful-firewall <a href="#">rule rule-name</a> <a href="#">term term-name</a> <a href="#">from</a> ]
Release Information	Statement introduced before Junos OS Release 7.4. <b>any-unicast</b> and <b>except</b> options introduced in Junos OS Release 7.6. <b>address</b> option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
Description	Specify the destination address for rule matching.
Options	<b>address</b> —Destination IPv4 or IPv6 address or prefix value. Using a value of 0::0/0 with IPv6 is not allowed for M-Series and MX-Series routers.  <b>any-unicast</b> —Match all unicast packets.  <b>except</b> —(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.
Usage Guidelines	See <a href="#">“Configuring Match Conditions in Stateful Firewall Rules” on page 389</a> .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## destination-address-range

---

Syntax	destination-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>;
Hierarchy Level	[edit <a href="#">services (stateful-firewall)</a> stateful-firewall <a href="#">rule rule-name</a> <a href="#">term term-name</a> <a href="#">from</a> ]
Release Information	Statement introduced in Junos OS Release 7.6. <b>minimum-value</b> and <b>maximum-value</b> options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
Description	Specify the destination address range for rule matching.
Options	<b>minimum-value</b> —Lower boundary for the IPv4 or IPv6 address range.  <b>maximum-value</b> —Upper boundary for the IPv4 or IPv6 address range.  <b>except</b> —(Optional) Exclude the specified address range from rule matching.
Usage Guidelines	See <a href="#">“Configuring Match Conditions in Stateful Firewall Rules” on page 389</a> .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## destination-prefix-list

---

<b>Syntax</b>	<code>destination-prefix-list <i>list-name</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[ <a href="#">edit services (stateful-firewall)</a> stateful-firewall <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	Specify the destination prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the [ <a href="#">edit policy-options</a> ] hierarchy level.
<b>Options</b>	<p><b><i>list-name</i></b>—Destination prefix list.</p> <p><b>except</b>—(Optional) Exclude the specified prefix list from rule matching.</p>
<b>Usage Guidelines</b>	See " <a href="#">Configuring Match Conditions in Stateful Firewall Rules</a> " on page 389.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Routing Policy Feature Guide for Routing Devices</i></li></ul>

## from

---

<b>Syntax</b>	<pre>from {   application-sets set-name;   applications [ application-names ];   destination-address (address   any-unicast) &lt;except&gt;;   destination-address-range low minimum-value high maximum-value &lt;except&gt;;   destination-prefix-list list-name &lt;except&gt;;   source-address (address   any-unicast) &lt;except&gt;;   source-address-range low minimum-value high maximum-value &lt;except&gt;;   source-prefix-list list-name &lt;except&gt;; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> stateful-firewall <a href="#">rule</a> rule-name <a href="#">term</a> term-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify input conditions for a stateful firewall term.
<b>Options</b>	<p>For information on match conditions, see the description of firewall filter match conditions in the <i>Routing Policy Feature Guide for Routing Devices</i>.</p> <p>The remaining statements are explained separately.</p>
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Stateful Firewall Rules</a> ” on page 388.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## match-direction

---

<b>Syntax</b>	<pre>match-direction (input   output   input-output);</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> stateful-firewall <a href="#">rule</a> rule-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the direction in which the rule match is applied.
<b>Options</b>	<p><b>input</b>—Apply the rule match on the input side of the interface.</p> <p><b>output</b>—Apply the rule match on the output side of the interface.</p> <p><b>input-output</b>—Apply the rule match bidirectionally.</p>
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Stateful Firewall Rules</a> ” on page 388.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## rule

<b>Syntax</b>	<pre> rule <i>rule-name</i> {   <b>match-direction</b> (input   output   input-output);   <b>term</b> <i>term-name</i> {     <b>from</b> {       <b>application-sets</b> <i>set-name</i>;       <b>applications</b> [ <i>application-names</i> ];       <b>destination-address</b> (<i>address</i>   any-unicast) &lt;except&gt;;       <b>destination-address-range</b> low <i>minimum-value</i> high <i>maximum-value</i> &lt;except&gt;;       <b>destination-prefix-list</b> <i>list-name</i> &lt;except&gt;;       <b>source-address</b> (<i>address</i>   any-unicast) &lt;except&gt;;       <b>source-address-range</b> low <i>minimum-value</i> high <i>maximum-value</i> &lt;except&gt;;       <b>source-prefix-list</b> <i>list-name</i> &lt;except&gt;;     }     <b>then</b> {       (accept   discard   reject);       <b>syslog</b>;     }   } } </pre>
<b>Hierarchy Level</b>	[edit <b>services</b> stateful-firewall], [edit <b>services</b> stateful-firewall <b>rule-set</b> <i>rule-set-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the rule the router uses when applying this service.
<b>Options</b>	<p><b><i>rule-name</i></b>—Identifier for the collection of terms that constitute this rule.</p> <p>The remaining statements are explained separately.</p>
<b>Usage Guidelines</b>	See “Configuring Stateful Firewall Rules” on page 388.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

## rule-set

---

<b>Syntax</b>	<code>rule-set <i>rule-set-name</i> {     [ <i>rule</i> <i>rule-names</i> ]; }</code>
<b>Hierarchy Level</b>	[edit <i>services</i> stateful-firewall]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<i>rule-set-name</i> —Identifier for the collection of rules that constitute this rule set.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Stateful Firewall Rule Sets</a> ” on page 392.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## services (stateful-firewall)

---

<b>Syntax</b>	<code>services stateful-firewall { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Define the service rules to be applied to traffic.
<b>Options</b>	<i>stateful-firewall</i> —Identifies the stateful firewall set of rules statements.
<b>Usage Guidelines</b>	See <i>Junos Network Secure</i> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## source-address

<b>Syntax</b>	<code>source-address (<i>address</i>   any-unicast) &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> stateful-firewall <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>any-unicast</b> and <b>except</b> options introduced in Junos OS Release 7.6. <b>address</b> option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Source address for rule matching.
<b>Options</b>	<b>address</b> —Source IPv4 or IPv6 address or prefix value.  <b>any-unicast</b> —Any unicast packet.  <b>except</b> —(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Match Conditions in Stateful Firewall Rules</a> ” on page 389.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## source-address-range

<b>Syntax</b>	<code>source-address-range low <i>minimum-value</i> high <i>maximum-value</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> stateful-firewall <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6. <b>minimum-value</b> and <b>maximum-value</b> options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Source address range for rule matching.
<b>Options</b>	<b>minimum-value</b> —Lower boundary for the IPv4 or IPv6 address range.  <b>maximum-value</b> —Upper boundary for the IPv4 or IPv6 address range.  <b>except</b> —(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Match Conditions in Stateful Firewall Rules</a> ” on page 389.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## source-prefix-list

---

<b>Syntax</b>	source-prefix-list <i>list-name</i> <except>;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> stateful-firewall <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	Specify the source prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the [edit <b>policy-options</b> ] hierarchy level.
<b>Options</b>	<i>list-name</i> —Destination prefix list.  <b>except</b> —(Optional) Exclude the specified prefix list from rule matching.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Match Conditions in Stateful Firewall Rules</a> ” on page 389.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Routing Policy Feature Guide for Routing Devices</i></li></ul>

## syslog

---

<b>Syntax</b>	syslog;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> stateful-firewall <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Enable system logging. The system log information from the Adaptive Services or Multiservices PIC is passed to the kernel for logging in the <b>/var/log</b> directory. This setting overrides any <b>syslog</b> statement setting included in the service set or interface default configuration.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in Stateful Firewall Rules on page 390</a></li></ul>

## term

```
Syntax  term term-name {
        from {
            application-sets set-name;
            applications [ application-names ];
            destination-address (address | any-unicast) <except>;
            destination-address-range low minimum-value high maximum-value <except>;
            destination-prefix-list list-name <except>;
            source-address (address | any-unicast) <except>;
            source-address-range low minimum-value high maximum-value <except>;
            source-prefix-list list-name <except>;
        }
        then {
            (accept | discard | reject);
            syslog;
        }
    }
```

**Hierarchy Level** [edit [services](#) stateful-firewall [rule](#) *rule-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the stateful firewall term properties.

**Options** *term-name*—Identifier for the term.

The remaining statements are explained separately.

**Usage Guidelines** See “[Configuring Stateful Firewall Rules](#)” on page 388.

**Required Privilege** interface—To view this statement in the configuration.

**Level** interface-control—To add this statement to the configuration.

## then

---

<b>Syntax</b>	<pre>then {     (accept   discard   reject);     syslog; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> stateful-firewall <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the stateful firewall term actions. You can configure the router to accept, discard, or reject the targeted traffic. The other actions are optional.
<b>Options</b>	<p><b>accept</b>—Accept the traffic and send it on to its destination.</p> <p><b>discard</b>—Do not accept traffic or process it further.</p> <p><b>reject</b>—Do not accept the traffic and return a rejection message. Rejected traffic can be logged or sampled.</p> <p>The remaining statement is explained separately.</p>
<b>Usage Guidelines</b>	See <a href="#">“Configuring Actions in Stateful Firewall Rules”</a> on page 390.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li><i>Routing Policy Feature Guide for Routing Devices</i></li></ul>

# Stateful Firewall on the Embedded Junos OS Platform Configuration Guidelines

Till now, all services run only on the Juniper microkernel software platform. However, some services will now be deployed on the Embedded Junos software platform. This allows such services to be coupled with third-party applications. Starting with Junos OS Release 9.5, the stateful firewall service has been implemented using the embedded Junos Application Framework (eJAF). The stateful firewall plug-in described in the following sections supports many of the features of the existing stateful firewall service that runs on the Juniper microkernel.

This chapter contains the following sections:

- [Loading the Stateful Firewall Plug-In on page 409](#)
- [Configuring Memory for the Stateful Firewall Plug-In on page 411](#)
- [Configuring rsh, rlogin, rexec for Stateful Firewall on page 411](#)

## Loading the Stateful Firewall Plug-In

---

As of Junos OS Release 9.5, a stateful firewall plug-in is provided as part of the jbundle package. To load this plug-in on the PIC, include the **package jservices-sfw** statement at the **[edit chassis fpc slot-number pic slot-number adaptive-services service-package extension-provider]** hierarchy level. For example:

```
user@host# show chassis
fpc 0 {
  pic 2 {
    adaptive-services {
      service-package {
        extension-provider {
          control-cores 1;
          data-cores 7;
          object-cache-size 512;
          package jservices-sfw; #Loads stateful firewall plug-in.
          policy-db-size 64;
        }
      }
    }
  }
}
```

You can load both the **jservices-sfw** package and a Junos SDK application package on the same PIC.

The following example demonstrates the stateful firewall plug-in coexisting with a provider's plug-in:

```
[edit]
services {
  service-set sset {
    stateful-firewall-rules rule1;
    interface-service {
      service-interface ms-0/0/0;
    }
    extension-service customer-plugin;
    service-order {
      forward-flow [ stateful-firewall customer-plugin ];
    }
  }
  stateful-firewall {
    rule rule1 {
      match-direction input-output;
      term term1 {
        from {
          applications junos-ftp;
        }
        then {
          accept;
        }
      }
    }
    rule rule2 {
      match-direction input;
      term term1 {
        from {
          source-address {
            192.1.1.2/32;
          }
        }
        then {
          reject;
          syslog;
        }
      }
    }
  }
}
```

The following stateful firewall operational commands support the **ms-** interface:

- **show services stateful-firewall flows**—Display stateful firewall flow table entries.
- **show services stateful-firewall statistics**—Display stateful firewall statistics. For this command, only rule and ALG statistics are given. In the extensive option, other statistics appear but do not populate correctly; those values are all zeroes.
- **clear services stateful-firewall flows**—Remove established flows from the flow table.

The commands are described in the [CLI Explorer](#).

- Related Documentation**
- [Configuring Memory for the Stateful Firewall Plug-In on page 411](#)
  - [extension-provider on page 416](#)

## Configuring Memory for the Stateful Firewall Plug-In

When configuring the stateful firewall internal plug-in, some questions remain regarding the upper limit to specify for the **policy-db-size**, **object-cache-size**, and **forwarding-db-size** statements when the application needs to use a large number of rules, causing the total memory required to approach the size of the object cache configured. The following limits, which are specific to the stateful firewall configuration, await additional review:

- Maximum number of terms (with one rule per term) per service set: 1200
- Maximum number of service sets per Multiservices PIC: 4000 (Juniper Networks M Series Multiservice Edge Routers and T Series Core Routers), 6000 (Juniper Networks MX Series 3D Universal Edge Routers and M120 Multiservice Edge Routers)
- Maximum object cache size: 1280 MB (Multiservices 400 PICs and DPCs), 512 MB (Multiservices 100 PICs)
- Maximum policy database size: Still to be determined.

If the policy database is set too small, an error message is logged in the router message file even though the commit may appear to be successful. It is necessary to check the logs to make sure that no message file error is found to be sure that the stateful firewall commit was indeed successful. The remedial action is to increase the size of the policy database.

- Related Documentation**
- [extension-provider on page 416](#)

## Configuring rsh, rlogin, rexec for Stateful Firewall

Some implementations of the rsh, rlogin, rexec mechanism require the remote host to authenticate the request by opening a separate TCP session to port 113 on the client host. By default, the stateful firewall does not allow this authentication flow to go through.

To open the authentication flow, include the **applications junos-ident** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* from]** hierarchy level:

```
[edit]
services {
  stateful-firewall {
    rule rule1 {
      term term1 {
        from {
          (source-address | destination-address);
          applications junos-ident;
        }
        then {
```

```
        accept;
      }
    }
  }
}
```

To allow Kerberos-enabled rsh, rlogin, rexec through the stateful firewall, configure the following additional applications and include them in the stateful firewall terms:

```
[edit]
applications {
  application test-kerberos-kshell {
    Protocol tcp;
    destination-port kshell;
  }
  application test kerberos-klogin {
    protocol tcp;
    destination-port klogin;
  }
}

services {
  stateful-firewall {
    rule rule1 {
      term term1 {
        from {
          applications [kerberos-klogin kerberos-kshell];
        }
        then {
          accept;
        }
      }
    }
  }
}
```

**Related Documentation**

- [Configuring Memory for the Stateful Firewall Plug-In on page 411](#)

## CHAPTER 14

# Summary of Stateful Firewall on the Embedded Junos OS Platform Configuration Statements

The following sections explain stateful firewall statements used in SDK applications. The statements are organized alphabetically.

### control-cores

---

<b>Syntax</b>	<code>control-cores control-number;</code>
<b>Hierarchy Level</b>	<code>[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Configure control cores. Any cores not configured as either control or data cores are treated as user cores. When the number of control cores is changed, the PIC reboots.
<b>Options</b>	<b>control-number</b> —Number of control cores. At least one core must be a control core. <b>Range:</b> 1 through 8
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Control and Data Cores</i></li><li>• <a href="#">data-cores on page 414</a></li></ul>

## data-cores

---

<b>Syntax</b>	<code>data-cores <i>data-number</i>;</code>
<b>Hierarchy Level</b>	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package <a href="#">extension-provider</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Configure data cores. Any cores not configured as either data or control cores are treated as user cores. When the number of data cores is changed, the PIC reboots.
<b>Options</b>	<b><i>data-number</i></b> —Number of data cores. Although it is not mandatory to dedicate any cores as data cores, it is advisable, depending on the nature of the application, to dedicate a minimum of five as data cores to achieve good performance. <b>Range:</b> 0 through 7
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Control and Data Cores</i></li><li>• <a href="#">control-cores on page 413</a></li></ul>

## data-flow-affinity

---

<b>Syntax</b>	<code>data-flow-affinity {     <a href="#">hash-key</a> (layer-3   layer-4); }</code>
<b>Hierarchy Level</b>	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package <a href="#">extension-provider</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Enable flow affinity distribution for packets over data CPUs on the PIC. Once enabled, the default behavior distributing data packets changes from a round-robin distribution to a flow affinity distribution based on a hash distribution. Adding or deleting this statement causes the PIC to reboot.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Packet Distribution Settings</i></li></ul>

## destination (Chassis)

---

<b>Syntax</b>	<code>destination <i>destination</i>;</code>
<b>Hierarchy Level</b>	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package extension-provider <a href="#">syslog facility</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	<p>Configure where log messages go. By default, all messages go to the <code>/var/log</code> directory on the Routing Engine. Enhancements to the existing infrastructure make debugging on the Multiservices PIC easier by giving the user the option of redirecting log messages. When the <b>syslog destination</b> statement is configured to redirect the log messages, you can use the <b>set system syslog</b> command, a command available in the native Junos OS CLI, to override the syslog settings made on the Multiservices PIC.</p>
<b>Options</b>	<p><b>destination</b>—Choose one of the following options:</p> <ul style="list-style-type: none"><li>• <b>routing-engine</b>—Forward log messages to the Routing Engine.</li><li>• <b>pic-console</b>—Forward log messages to the console of the PIC.</li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Log Messages</a></li><li>• <a href="#">extension-provider on page 416</a></li></ul>

## extension-provider

---

**Syntax**    `extension-provider {  
              control-cores control-number;  
              data-cores data-number;  
              data-flow-affinity {  
                  hash-key (layer-3 | layer-4);  
              }  
              forwarding-db-size size;  
              object-cache-size size;  
              package package-name;  
              policy-db-size size;  
              syslog {  
                  facility {  
                      severity;  
                      destination destination;  
                  }  
              }  
              wired-max-processes num-procs;  
              wired-process-mem-size mem-size;  
          }`

**Hierarchy Level**    `[edit chassis fpc slot-number pic pic-number adaptive-services service-package]`

**Release Information**    Statement introduced in Junos OS Release 9.0.

**Description**    Configure an application on a PIC. When the **extension-provider** statement is first configured, the PIC reboots.


The statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring Control and Data Cores*
- *Configuring Packet Distribution Settings*
- *Configuring Memory Settings*
- *Configuring Packages on the PIC*
- *Configuring System Log Messages*

## forwarding-db-size

<b>Syntax</b>	forwarding-db-size <i>size</i> ;
<b>Hierarchy Level</b>	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package <a href="#">extension-provider</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the size of the forwarding database (FDB). When this setting is changed, the PIC reboots.
<div>  <b>NOTE:</b> You need to enable the <code>forwarding-options sampling</code> statement for the FDB to be created. </div>	
<b>Options</b>	<p><b>size</b>—Size of the FDB, in megabytes (MB). The size of the FDB and the size of the policy database together must be smaller than the size of the object cache.</p> <p><b>Range:</b> 0 through 12879 MB</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Memory Settings</a></li> <li>• <a href="#">policy-db-size on page 421</a></li> <li>• <a href="#">wired-process-mem-size on page 423</a></li> <li>• <a href="#">object-cache-size on page 419</a></li> </ul>

## hash-key (Chassis)

---

<b>Syntax</b>	hash-key (layer-3   layer-4);
<b>Hierarchy Level</b>	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package extension-provider <a href="#">data-flow-affinity</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Set the hashing distribution of flow affinity. This is an optional setting. Once the <b>data-flow-affinity</b> statement is enabled, you may need to choose the hashing distribution. Modifying this statement causes the PIC to reboot.
<b>Default</b>	If you do not configure the <b>hash-key</b> statement, the hashing distribution is 5-tuple hashing, or <b>layer-4</b> .
<b>Options</b>	<b>layer-3</b> —3-tuple hashing (source IP address, destination IP address, and IP protocol). <b>layer-4</b> —5-tuple hashing (3-tuple plus source and destination TCP or UDP ports).
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Packet Distribution Settings</i></li><li>• <a href="#">extension-provider on page 416</a></li></ul>

## object-cache-size

---

<b>Syntax</b>	<code>object-cache-size value;</code>
<b>Hierarchy Level</b>	<code>[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Configure the size of the object cache. When this setting is changed, the PIC reboots.
<b>Options</b>	<p><b>value</b>—Amount of object cache, in MB. Only values in increments of 128 MB are allowed.</p> <p><b>Range:</b> For Multiservices 100 PIC, range is 128 MB through 512 MB. If the <b>wired-process-mem-size</b> statement at the same hierarchy level has a value of 512 MB, the maximum value for this statement is 128 MB.</p> <p><b>Range:</b> For Multiservices 400 PIC, range is 128 MB through 1280 MB. If the <b>wired-process-mem-size</b> statement at the same hierarchy level has a value of 512 MB, the maximum value for this statement is 512 MB.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Memory Settings</i></li><li>• <a href="#">forwarding-db-size on page 417</a></li><li>• <a href="#">policy-db-size on page 421</a></li><li>• <a href="#">wired-process-mem-size on page 423</a></li></ul>

## package (Loading on PIC)

---

<b>Syntax</b>	<code>package <i>package-name</i>;</code>
<b>Hierarchy Level</b>	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package <a href="#">extension-provider</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Identify a package to be loaded on the PIC. When a package is added or removed, the PIC reboots.
<b>Options</b>	<b><i>package-name</i></b> —Name of the package to be loaded on the PIC. There can be up to eight packages loaded on a PIC; however, only one data package is allowed per PIC. An error message is displayed if more than eight packages are specified.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Packages on the PIC</i></li></ul>

## policy-db-size

<b>Syntax</b>	<code>policy-db-size size;</code>
<b>Hierarchy Level</b>	<code>[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the size of the policy database. When this setting is changed, the PIC reboots.



**NOTE:** At least one data core must be configured to configure the size of the policy database.

<b>Options</b>	<p><b>size</b>—Size of the policy database, in megabytes (MB). The size of the forwarding database and the size of the policy database together must be smaller than the size of the object cache.</p> <p><b>Range:</b> 0 through 1279 MB</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Memory Settings</i></li> <li>• <a href="#">forwarding-db-size on page 417</a></li> <li>• <a href="#">object-cache-size on page 419</a></li> <li>• <a href="#">wired-process-mem-size on page 423</a></li> </ul>

## syslog (Chassis)

---

Syntax	<pre>syslog {     facility {         severity;         destination destination;     } }</pre>
Hierarchy Level	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package <i>extension-provider</i> ]
Release Information	Statement introduced in Junos OS Release 9.2. Options <b>daemon</b> and <b>kernel</b> (for <i>facility</i> ) introduced in Junos OS Release 9.5.
Description	Enable PIC system logging to record or view system log messages on a specific PIC. The system log information is passed to the kernel for logging in the <b>/var/log</b> directory.
Options	<p><b>facility</b>—Group of messages that are either generated by the same software process or concern a similar condition or activity. Possible values include the following: <b>daemon</b>, <b>external</b>, <b>kernel</b>, and <b>pfe</b>.</p> <p><b>severity</b>—Classification of effect on functioning. Possible values are the following options:</p> <ul style="list-style-type: none"><li>• <b>any</b>—Include all severity levels.</li><li>• <b>none</b>—Disable logging of the associated facility to a destination.</li><li>• <b>emergency</b>—System panic or other condition that causes the routing platform to stop functioning.</li><li>• <b>alert</b>—Conditions that require immediate correction, such as a corrupted system database.</li><li>• <b>critical</b>—Critical conditions, such as hard errors.</li><li>• <b>error</b>—Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.</li><li>• <b>warning</b>—Conditions that warrant monitoring.</li><li>• <b>notice</b>—Conditions that are not errors but might warrant special handling.</li><li>• <b>info</b>—Events or nonerror conditions of interest.</li></ul> <p>The remaining statement is explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring System Log Messages</i></li></ul>

## wired-process-mem-size

---

<b>Syntax</b>	wired-process-mem-size <i>mem-size</i> ;
<b>Hierarchy Level</b>	[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package <a href="#">extension-provider</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the size of the reserved wired process memory. You can also configure object cache. If this setting is changed, the PIC reboots.
<b>Options</b>	<b>megabytes</b> —Size of the reserved wired process memory, in MB. The only size you can set for this statement is 512 MB. <b>Default:</b> 512 MB <b>Range:</b> 0 through 512 MB
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Memory Settings</i></li><li>• <a href="#">forwarding-db-size on page 417</a></li><li>• <a href="#">object-cache-size on page 419</a></li><li>• <a href="#">policy-db-size on page 421</a></li><li>• <b>wired-max-processes</b></li></ul>



# Load Balancing Configuration Guidelines

As of now, most router services are provisioned using service sets in Junos OS. Each service set directs traffic to a specific preconfigured services PIC only. This leads to inefficient use of networking resources within a system. Load balancing resolves this situation by allowing distribution of ingress and egress traffic across multiple services PICs. Load balancing works by hashing each packet and then redirecting the packet to the appropriate services PIC. Load balancing can be accomplished only on MX Series 3D Universal Edge routers because services PICs require symmetric hashing to ensure that ingress and egress traffic are directed properly.

- [Configuring Load Balancing on AMS Infrastructure on page 425](#)
- [Example: Configuring Static Source Translation on AMS Infrastructure on page 427](#)

## Configuring Load Balancing on AMS Infrastructure

---

Configuring load balancing requires an aggregated Multiservices (AMS) system. AMS involves grouping several Multiservices PICs together. An AMS configuration eliminates the need for separate routers within a system. The primary benefit of having an AMS configuration is the ability to support load balancing of traffic across multiple services PICs.



**NOTE:** AMS is supported only on Mobility Gateway (MBG) with the MBG MS-DPC. AMS is not supported with JUNOS services like NAT, FW, IPsec, DAA, HCM on the current MS-DPC.

Starting with Junos OS 11.4, high availability (HA) is supported on AMS infrastructure on all MX Series 3D Universal Edge routers. AMS has several benefits:

- Support for configuring behavior if a Multiservices PIC that is part of the AMS configuration fails
- Support for specifying hash keys for each service set in either direction
- Support for adding routes to individual PICs within the AMS system

## Configuring AMS Infrastructure

AMS supports load balancing across multiple service sets. All ingress or egress traffic for a service set can be load balanced across different services PICs. To enable load balancing, you have to configure an aggregate interface with existing services interfaces.

To configure failure behavior in AMS, include the **member-failure-options** statement:

```
[edit interfaces ams1]
load-balancing-options {
  member-failure-options {
    drop-member-traffic {
      rejoin-timeout rejoin-timeout;
    }
    redistribute-all-traffic {
      enable-rejoin;
    }
  }
}
```

If a PIC fails, the traffic to the failed PIC can be configured to be redistributed by using the **redistribute-all-traffic** statement at the **[edit interfaces *interface-name* load-balancing-options member-failure-options]** hierarchy level. If the **drop-member-traffic** statement is used, all traffic to the failed PIC is dropped. Both options are mutually exclusive.



**NOTE:** If **member-failure-options** is not explicitly configured, the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

Only **mams-** interfaces (services interfaces that are part of AMS) can be aggregated. After an AMS interface has been configured, the constituent **mams-** interfaces cannot be individually configured. A **mams-** interface cannot be used as an **rms** interface. AMS supports only IPv4; inet6 family is not supported. It is not possible to configure addresses on an AMS interface. Network Address Translation (NAT) is the only application that runs on AMS infrastructure at this time.



**NOTE:** Unit 0 on an AMS interface cannot be configured.

To support multiple applications and different types of translation, AMS infrastructure supports configuring hashing for each service set. The hash keys can be configured separately for ingress and egress. The default configuration uses source IP, destination IP, and the protocol for hashing; incoming-interface for ingress and outgoing-interface for egress are also available.

## Configuring High Availability

In an AMS system configured with high availability, a designated Multiservices PIC acts as a backup for other active PICs that are part of the AMS system. Presently, only N:1 backup for high availability is supported; only one PIC is available as backup for all other

active PICs. High availability for load balancing is configured by adding the **high-availability-options** statement at the **[edit interfaces *interface-name* load-balancing-options]** hierarchy level.

To configure high availability, include the **high-availability-options** statement:

```
[edit interfaces ams1]
load-balancing-options {
  high-availability-options {
    many-to-one {
      preferred-backup preferred-backup;
    }
  }
}
```

## Load Balancing Network Address Translation Flows

Starting with Junos OS Release 11.4, Network Address Translation (NAT) has been programmed as a plug-in and is a function of load balancing and high availability. The plug-in runs on AMS infrastructure. All flows for translation are automatically distributed to different services PICs that are part of the AMS infrastructure. In case of failure of an active Multiservices PIC, the configured backup Multiservices PIC will take over the NAT pool resources of the failed PIC. The hashing method selected depends on the type of NAT. Using NAT on AMS infrastructure has a few limitations:

- NAT flows to failed PICs cannot be restored.
- There is no support for IPv6 flows.
- Twice NAT is not supported for load balancing.

See “[Example: Configuring Static Source Translation on AMS Infrastructure](#)” on page 427 for more details on configuring NAT flows for load balancing.

### Related Documentation

- [Understanding Aggregated Multiservices Interfaces on page 93](#)
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\) on page 94](#)
- [Example: Configuring Next-Hop Style Services on an Aggregated Multiservices Interface on page 99](#)
- [Example: Configuring Static Source Translation on AMS Infrastructure on page 427](#)

## Example: Configuring Static Source Translation on AMS Infrastructure

This example shows a static source translation configured on an AMS interface. The flows will be load balanced across member interfaces with this example.

Configure the AMS interface **ams0** with load balancing options.

```
[edit interfaces ams0]
load-balancing-options {
  member-interface mams-5/0/0;
  member-interface mams-5/1/0;
```

```
}
unit 1 {
    family inet;
}
unit 2 {
    family inet;
}
```

Configure hashing for the service set for both ingress and egress traffic.

```
[edit services service-set ss1]
interface-service {
    service-interface ams0.1;
    load-balancing-options {
        hash-keys {
            ingress-key destination-ip;
            egress-key source-ip;
        }
    }
}
```



**NOTE:** Hashing is determined based on whether the service set is applied on the ingress or egress interface.

---

Configure two NAT pools because you have configured two member interfaces for the AMS interface.

```
[edit services]
nat {
    pool p1 {
        address-range low 20.1.1.80 high 20.1.1.80;
    }
    pool p2 {
        address 20.1.1.81/32;
    }
}
```

Configure the NAT rule and translation.

```
[edit services]
nat {
    rule r1 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    20.1.1.2/32;
                }
            }
            then {
                translated {
                    source-pool p1;
                    translation-type {
                        basic-nat44;
                    }
                }
            }
        }
    }
}
```

```
    }  
    term t1 {  
        from {  
            source-address {  
                40.1.1.2/32;  
            }  
        }  
        then {  
            translated {  
                source-pool p2;  
                translation-type {  
                    basic-nat44;  
                }  
            }  
        }  
    }  
}
```



**NOTE:** A similar configuration can be applied for translation types `dynamic-nat44` and `napt-44`. Twice NAT cannot run on AMS infrastructure at this time.

**Related  
Documentation**

- [Configuring Load Balancing on AMS Infrastructure on page 425](#)
- [Understanding Aggregated Multiservices Interfaces on page 93](#)



# Summary of Load Balancing Configuration Statements

The following sections explain each of the load balancing and aggregated Multiservices (AMS) statements. The statements are organized alphabetically.

- [drop-member-traffic \(Aggregated Multiservices\) on page 432](#)
- [enable-rejoin \(aggregated Multiservices\) on page 433](#)
- [family \(aggregated Multiservices\) on page 433](#)
- [high-availability-options \(aggregated Multiservices\) on page 434](#)
- [interfaces \(Aggregated Multiservices\) on page 435](#)
- [load-balancing-options \(Aggregated Multiservices\) on page 436](#)
- [many-to-one \(Aggregated Multiservices\) on page 437](#)
- [member-failure-options \(Aggregated Multiservices\) on page 438](#)
- [member-interface \(Aggregated Multiservices\) on page 440](#)
- [redistribute-all-traffic \(Aggregated Multiservices\) on page 441](#)
- [rejoin-timeout \(Aggregated Multiservices\) on page 442](#)
- [unit \(Aggregated Multiservices\) on page 443](#)

## drop-member-traffic (Aggregated Multiservices)

---

<b>Syntax</b>	<pre>drop-member-traffic {     <i>rejoin-timeout</i> <i>rejoin-timeout</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	<p>Specify whether the broadband gateway should drop traffic to a Multiservices PIC when it fails.</p> <p>For many-to-one (N:1) high availability (HA) for service applications like Network Address Translation (NAT), this configuration is valid only when two or more Multiservices PICs have failed.</p> <p>The remaining statement is explained separately.</p>
<b>Default</b>	If this statement is not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">member-failure-options (Aggregated Multiservices) on page 438</a></li><li>• <a href="#">Understanding Aggregated Multiservices Interfaces on page 93</a></li><li>• <a href="#">Example: Configuring an Aggregated Multiservices Interface (AMS) on page 94</a></li></ul>

## enable-rejoin (aggregated Multiservices)

<b>Syntax</b>	enable-rejoin;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options redistribute-all-traffic]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	<p>Enable the failed member to rejoin the aggregated Multiservices (AMS) interface after the member comes back online.</p> <p>For many-to-one (N:1) high availability (HA) for service applications like Network Address Translation (NAT), this configuration allows the failed members to rejoin the pool of active members automatically.</p>
<b>Default</b>	If you do not configure this option, then the failed members do not automatically rejoin the <b>ams</b> interface even after coming back online.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">redistribute-all-traffic (Aggregated Multiservices) on page 441</a></li> <li>• <a href="#">Understanding Aggregated Multiservices Interfaces on page 93</a></li> <li>• <a href="#">Example: Configuring an Aggregated Multiservices Interface (AMS) on page 94</a></li> </ul>

## family (aggregated Multiservices)

<b>Syntax</b>	family <i>family</i> ;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Configure protocol family information for the logical interface.
<b>Options</b>	<b>family</b> —Protocol family. Currently, only one option, <b>inet</b> (IP version 4 suite), is supported.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">unit (Aggregated Multiservices) on page 443</a></li> <li>• <a href="#">Understanding Aggregated Multiservices Interfaces on page 93</a></li> <li>• <a href="#">Example: Configuring an Aggregated Multiservices Interface (AMS) on page 94</a></li> </ul>

## high-availability-options (aggregated Multiservices)

---

**Syntax**    high-availability-options {  
              many-to-one {  
                  preferred-backup *preferred-backup*;  
              }  
          }

**Hierarchy Level**    [edit interfaces *interface-name* load-balancing-options]

**Release Information**    Statement introduced in Junos OS Release 11.4.

**Description**    Configure the high availability options for the aggregated Multiservices (AMS) interface. For service applications, if only the load-balancing feature is being used, then this configuration is optional.

For many-to-one (N:1) high availability support for service applications like Network Address Translation (NAT), the preferred backup Multiservices PIC, in hot standby mode, backs up one or more (N) active Multiservices PICs.



**NOTE:** In both cases, if one of the active Multiservices PICs goes down, then the backup replaces it as the active Multiservices PIC. When the failed PIC comes back up, it becomes the new backup. This is called floating backup.

---

The remaining statements are explained separately.

**Required Privilege**    interface—To view this statement in the configuration.  
**Level**    interface-control—To add this statement to the configuration.

**Related Documentation**

- [load-balancing-options on page 436](#)
- [Understanding Aggregated Multiservices Interfaces on page 93](#)
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\) on page 94](#)

## interfaces (Aggregated Multiservices)

```
Syntax  interfaces interface-name {
        load-balancing-options {
            high-availability-options {
                many-to-one {
                    preferred-backup preferred-backup;
                }
            }
            member-failure-options {
                drop-member-traffic {
                    rejoin-timeout rejoin-timeout;
                }
                redistribute-all-traffic {
                    enable-rejoin;
                }
            }
            member-interface interface-name;
        }
        unit interface-unit-number {
            family family;
        }
    }
```

Hierarchy Level [\[edit\]](#)

**Release Information** Statement introduced in Junos OS Release 11.4.

**Description** Configure the aggregated Multiservices (AMS) interface. The AMS interface provides the infrastructure for load balancing and high availability (HA).



**NOTE:** The interfaces must be valid aggregated Multiservices interfaces (ams)—for example, ams0 or ams1, and so on. The ams infrastructure is supported only in chassis with Trio-based modules and Multiservices Dense Port Concentrators (MS-DPCs).

The remaining statements are explained separately.

**Options** **interface-name**—Name of the aggregated Multiservices interface (**ams**)—for example, ams0 or ams1, and so on.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Load Balancing on AMS Infrastructure on page 425](#)
- [Understanding Aggregated Multiservices Interfaces on page 93](#)
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\) on page 94](#)

## load-balancing-options (Aggregated Multiservices)

---

**Syntax**

```
load-balancing-options {  
  high-availability-options {  
    many-to-one {  
      preferred-backup preferred-backup;  
    }  
  }  
  member-failure-options {  
    drop-member-traffic {  
      rejoin-timeout rejoin-timeout;  
    }  
    redistribute-all-traffic {  
      enable-rejoin;  
    }  
  }  
  member-interface interface-name;  
}
```

**Hierarchy Level** [edit interfaces *interface-name*]

**Release Information** Statement introduced in Junos OS Release 11.4.

**Description** Configure the high availability (HA) options for the aggregated Multiservices (AMS) interface.

Many-to-one (N:1) high availability mode for service applications like Network Address Translation (NAT) is supported. In this case, one Multiservices PIC is the backup (in hot standby mode) for one or more (N) active Multiservices PICs. If one of the active Multiservices PICs goes down, then the backup replaces it as the active Multiservices PIC. When the failed PIC comes back online, it becomes the new backup. This is called floating backup mode.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [interfaces on page 435](#)
- [Understanding Aggregated Multiservices Interfaces on page 93](#)
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\) on page 94](#)

## many-to-one (Aggregated Multiservices)

<b>Syntax</b>	<code>many-to-one {     preferred-backup <i>preferred-backup</i>; }</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> load-balancing-options high-availability-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Configure the initial preferred backup for the aggregated Multiservices (AMS) interface.



**NOTE:** The preferred backup must be one of the member interfaces (*mams-*) that have already been configured at the [edit interfaces *interface-name* load-balancing-options] hierarchy level. Even in the case of mobile control plane redundancy, which is one-to-one (1:1), the initial preferred backup is configured at this hierarchy level.

The remaining statements are explained separately.

<b>Options</b>	<p><b>preferred-backup <i>preferred-backup</i></b>—Name of the preferred backup member interface. The member interface format is <b>mams-a/b/0</b>, where <b>a</b> is the Flexible PIC Concentrator (FPC) slot number and <b>b</b> is the PIC slot number.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">high-availability-options (aggregated Multiservices) on page 434</a></li> <li>• <a href="#">Understanding Aggregated Multiservices Interfaces on page 93</a></li> <li>• <a href="#">Example: Configuring an Aggregated Multiservices Interface (AMS) on page 94</a></li> </ul>

## member-failure-options (Aggregated Multiservices)

**Syntax**

```
member-failure-options {
  drop-member-traffic {
    rejoin-timeout rejoin-timeout;
  }
  redistribute-all-traffic {
    enable-rejoin;
  }
}
```

**Hierarchy Level** [edit interfaces *interface-name* load-balancing-options]

**Release Information** Statement introduced in Junos OS Release 11.4.

**Description** Configure the possible behavior for the aggregated Multiservices (AMS) interface in case of failure of more than one active member.



**NOTE:** The `drop-member-traffic` configuration and the `redistribute-all-traffic` configuration are mutually exclusive.

[Table 27 on page 438](#) displays the behavior of the member interface after the failure of the first Multiservices PIC. [Table 28 on page 439](#) displays the behavior of the member interface after the failure of two Multiservices PICs.



**NOTE:** The AMS infrastructure has been designed to handle one failure automatically. However, in the unlikely event that more than one Multiservices PIC fails, the AMS infrastructure provides configuration options to minimize the impact on existing traffic flows.

**Table 27: Behavior of Member Interface After One Multiservices PIC Fails**

High Availability Mode	Member Interface Behavior
Many-to-one (N:1) high availability support for service applications	Automatically handled by the AMS infrastructure

Table 28: Behavior of Member Interface After Two Multiservices PICs Fail

High Availability Mode	Configuration	rejoin-timeout	Behavior when member rejoins before rejoin-timeout expires	Behavior when member rejoins after rejoin-timeout expires
Many-to-one (N:1) high availability support for service applications	<b>drop-member-traffic</b>	Configured	<p>The existing traffic for the second failed member will <i>not</i> be redistributed to the other members.</p> <p>The first member to rejoin becomes an active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.</p>	<p>The existing traffic for the second failed member will <i>not</i> be redistributed to the other members.</p> <p>The first member will rejoin the AMS automatically. However, the other members who are rejoining will be moved to the discard state.</p>
Many-to-one (N:1) high availability support for service applications	<b>redistribute-all-traffic</b>	Not applicable	<p>Before rejoin, the traffic is redistributed to existing active members.</p> <p>After a failed member rejoins, the traffic is load-balanced afresh. This may impact existing traffic flows.</p>	

The remaining statements are explained separately.

**Default** If **member-failure-options** are not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.


**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [load-balancing-options \(Aggregated Multiservices\) on page 436](#)
- [Understanding Aggregated Multiservices Interfaces on page 93](#)
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\) on page 94](#)

## member-interface (Aggregated Multiservices)

---

<b>Syntax</b>	<code>member-interface <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> load-balancing-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	<p>Specify the member interfaces for the aggregated Multiservices (AMS) interface. You can configure multiple interfaces by specifying each interface in a separate statement.</p> <p>For high availability service applications like Network Address Translation (NAT) that support many-to-one (N:1) redundancy, you can specify two or more interfaces.</p>
	<div> <b>NOTE:</b> The member interfaces that you specify must be members of aggregated Multiservices interfaces (mams-).</div>
	<p>The remaining statements are explained separately.</p>
<b>Options</b>	<p><i>interface-name</i>—Name of the member interface. The member interface format is <b>mams-a/b/0</b>, where <b>a</b> is the Flexible PIC Concentrator (FPC) slot number and <b>b</b> is the PIC slot number.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding Aggregated Multiservices Interfaces on page 93</a></li><li>• <a href="#">Example: Configuring an Aggregated Multiservices Interface (AMS) on page 94</a></li><li>• <a href="#">load-balancing-options (Aggregated Multiservices) on page 436</a></li></ul>

## redistribute-all-traffic (Aggregated Multiservices)

---

<b>Syntax</b>	<code>redistribute-all-traffic {     enable-rejoin; }</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	<p>Enable the option to redistribute traffic of a failed active member to the other active members.</p> <p>For many-to-one (N:1) high availability support for Network Address Translation (NAT), the traffic for the failed member is automatically redistributed to the other active members.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding Aggregated Multiservices Interfaces on page 93</a></li><li>• <a href="#">Example: Configuring an Aggregated Multiservices Interface (AMS) on page 94</a></li><li>• <a href="#">member-failure-options (Aggregated Multiservices) on page 438</a></li></ul>

## rejoin-timeout (Aggregated Multiservices)

---

<b>Syntax</b>	<code>rejoin-timeout <i>rejoin-timeout</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options drop-member-traffic]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Configure the time by when a failed member should rejoin the aggregated Multiservices (AMS) interface automatically. If the failed member does not rejoin by the configured time, then the member is moved to the “inactive” state and the traffic meant for this member is dropped.
<b>Default</b>	If you do not configure a value, the default value of 120 seconds is used.
<b>Options</b>	<b><i>rejoin-timeout</i></b> —Time, in seconds, by which a failed member must rejoin. <b>Default:</b> 120 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding Aggregated Multiservices Interfaces on page 93</a></li><li>• <a href="#">Example: Configuring an Aggregated Multiservices Interface (AMS) on page 94</a></li><li>• <a href="#">drop-member-traffic (Aggregated Multiservices) on page 432</a></li></ul>

## unit (Aggregated Multiservices)

**Syntax**    `unit interface-unit-number {  
                  family family;  
                  }`

**Hierarchy Level**    [edit interfaces *interface-name*]

**Release Information**    Statement introduced in Junos OS Release 11.4.

**Description**    Configure the logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

The remaining statements are explained separately.

**Options**    *interface-unit-number*—Number of the logical unit.



**NOTE:** Unit 0 is reserved and cannot be configured under the aggregated Multiservices interface (ams).

**Range:** 1 through 16,384

**Required Privilege Level**    interface—To view this statement in the configuration.  
   interface-control—To add this statement to the configuration.

**Related Documentation**

- [Understanding Aggregated Multiservices Interfaces on page 93](#)
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\) on page 94](#)
- [interfaces on page 435](#)



# Intrusion Detection Service Configuration Guidelines

The Adaptive Services (AS) or Multiservices PIC supports a limited set of intrusion detection services (IDS) to perform attack detection. You can use IDS to perform the following tasks:

- Detect various types of denial-of-service (DoS) and directed denial-of-service (DDoS) attacks.
- Detect attempts at network scanning and probing.
- Detect anomalies in traffic patterns, such as sudden bursts or a decline in bandwidth.
- Prevent some types of attacks.
- Redirect attack traffic to a collector for analysis.
- Specify thresholds for limiting the number of flows, the packet rate, and the session rate.

IDS enables you to focus attack detection and remedial actions on specific hosts or networks that you specify in the IDS terms. Signature detection is not supported.

To configure IDS, include the **ids** statement at the **[edit services]** hierarchy level:

```
[edit services]
ids {
  rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
      rule {
        application-sets set-name;
        applications [ application-names ];
        destination-address (address | any-unicast) <except>;
        destination-address-range low minimum-value high maximum-value <except>;
        destination-prefix-list list-name <except>;
        source-address (address | any-unicast) <except>;
        source-address-range low minimum-value high maximum-value <except>;
        source-prefix-list list-name <except>;
      }
      then {
        aggregation {
```

```

        destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
        source-prefix prefix-value | source-prefix-ipv6 prefix-value;
    }
    (force-entry | ignore-entry);
    logging {
        syslog;
        threshold rate;
    }
    session-limit {
        by-destination {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
        }
        by-pair {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
        }
        by-source {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
        }
    }
    syn-cookie {
        mss value;
        threshold rate;
    }
}
}
}
rule-set rule-set-name {
    [ rule rule-names ];
}
}

```



**NOTE:** The Junos OS uses stateful firewall settings as a basis for performing IDS. You must commit a stateful firewall configuration in the same service set for IDS to function properly.

This chapter contains the following sections:

- [Configuring IDS Rules on page 447](#)
- [Configuring IDS Rule Sets on page 453](#)
- [Examples: Configuring IDS Rules on page 454](#)

## Configuring IDS Rules

IDS rules identify traffic for which you want the router software to count events. Because IDS is based on stateful firewall properties, you must configure at least one stateful firewall rule and include it in the service set with the IDS rules; for more information, see [“Configuring Stateful Firewall Rules” on page 388](#).

To configure an IDS rule, include the **rule** *rule-name* statement at the **[edit services ids]** hierarchy level:

```
[edit services ids]
rule rule-name {
  match-direction (input | output | input-output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address (address | any-unicast) <except>;
      destination-address-range low minimum-value high maximum-value <except>;
      destination-prefix-list list-name <except>;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
      source-prefix-list list-name <except>;
    }
    then {
      aggregation {
        destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
        source-prefix prefix-value | source-prefix-ipv6 prefix-value;
      }
      (force-entry | ignore-entry);
      logging {
        syslog;
        threshold rate;
      }
      session-limit {
        by-destination {
          hold-time seconds;
          maximum number;
          packets number;
          rate number;
        }
        by-pair {
          hold-time seconds;
          maximum number;
          packets number;
          rate number;
        }
        by-source {
          hold-time seconds;
          maximum number;
          packets number;
          rate number;
        }
      }
    }
  }
}
```

```
syn-cookie {  
  mss value;  
  threshold rate;  
}  
}  
}
```

Each IDS rule consists of a set of terms, similar to a filter configured at the **[edit firewall]** hierarchy level. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software.

The following sections describe IDS rule content in more detail:

- [Configuring Match Direction for IDS Rules on page 448](#)
- [Configuring Match Conditions in IDS Rules on page 449](#)
- [Configuring Actions in IDS Rules on page 450](#)

## Configuring Match Direction for IDS Rules

Each rule must include a **match-direction** statement that specifies whether the match is applied on the input or output side of the interface. To configure where the match is applied, include the **match-direction (input | input-output | output)** statement at the **[edit services ids rule rule-name]** hierarchy level:

```
[edit services ids rule rule-name]  
match-direction (input | output | input-output);
```

If you configure **match-direction input-output**, bidirectional rule creation is allowed.

The match direction is used with respect to the traffic flow through the AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.

With a next-hop service set, packet direction is determined by the interface used to route the packet to the AS or Multiservices PIC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the PIC, the packet direction is output. For more information on inside and outside interfaces, see [“Configuring Service Sets to be Applied to Services Interfaces” on page 742](#).

On the AS or Multiservices PIC, a flow lookup is performed. If no flow is found, rule processing is performed. All rules in the service set are considered. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that match the packet direction are considered.

## Configuring Match Conditions in IDS Rules

To configure IDS match conditions, include the **from** statement at the **[edit services ids rule rule-name term term-name]** hierarchy level:

```
[edit services ids rule rule-name term term-name]
from {
  application-sets set-name;
  applications [ application-names ];
  destination-address (address | any-unicast) <except>;
  destination-address-range low minimum-value high maximum-value <except>;
  destination-prefix-list list-name <except>;
  source-address (address | any-unicast) <except>;
  source-address-range low minimum-value high maximum-value <except>;
  source-prefix-list list-name <except>;
}
```

If you omit the **from** statement, the software accepts all events and places them in the IDS cache for processing.

The source address and destination address can be either IPv4 or IPv6. You can use the destination address, a range of destination addresses, a source address, or a range of source addresses as a match condition, in the same way that you would configure a firewall filter; for more information, see the *Routing Policy Feature Guide for Routing Devices*.

Alternatively, you can specify a list of source or destination prefixes by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either the **destination-prefix-list** or **source-prefix-list** statement in the IDS rule. For an example, see “Examples: Configuring Stateful Firewall Rules” on page 392.

You can also include application protocol definitions that you have configured at the **[edit applications]** hierarchy level; for more information, see “Configuring Application Protocol Properties” on page 146.

- To apply one or more specific application protocol definitions, include the **applications** statement at the **[edit services ids rule rule-name term term-name from]** hierarchy level.
- To apply one or more sets of application protocol definitions that you have defined, include the **application-sets** statement at the **[edit services ids rule rule-name term term-name from]** hierarchy level.



**NOTE:** If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the **[edit applications]** hierarchy level; you cannot specify these properties as match conditions.

If a match occurs on an application, the application protocol is displayed separately in the **show services ids** command output. For more information, see the [CLI Explorer](#).

## Configuring Actions in IDS Rules

To configure IDS actions, include the **then** statement at the **[edit services ids rule *rule-name* term *term-name*]** hierarchy level:

```
[edit services ids rule rule-name term term-name]
then {
  aggregation {
    destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
    source-prefix prefix-value | source-prefix-ipv6 prefix-value;
  }
  (force-entry | ignore-entry);
  logging {
    syslog;
    threshold rate;
  }
  session-limit {
    by-destination {
      hold-time seconds;
      maximum number;
      packets number;
      rate number;
    }
    by-pair {
      hold-time seconds;
      maximum number;
      packets number;
      rate number;
    }
    by-source {
      hold-time seconds;
      maximum number;
      packets number;
      rate number;
    }
  }
  syn-cookie {
    mss value;
    threshold rate;
  }
}
```

You can configure the following possible actions:

- **aggregation**—The router aggregates traffic labeled with the specified source or destination prefixes before passing the events to IDS processing. This is helpful if you want to examine all the traffic connected with a particular source or destination host. To collect traffic with some other marker, such as a particular application or port, configure that value in the match conditions.

To configure aggregation prefixes, include the **aggregation** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level and specify values for **source-prefix**, **destination-prefix**, **source-prefix-ipv6**, or **destination-prefix-ipv6**:

```
[edit services ids rule rule-name term term-name then]
```

```

aggregation {
  destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
  source-prefix prefix-value | source-prefix-ipv6 prefix-value;
}

```

The value of **source-prefix** and **destination-prefix** must be an integer between 1 and 32. The value of **source-prefix-ipv6** and **destination-prefix-ipv6** must be an integer between 1 and 128.

- **(force-entry | ignore-entry)**—**force-entry** provides a permanent spot in IDS caches for subsequent events after one event is registered. By default, the IDS software does not record information about “good” packets that do not exhibit suspicious behavior. You can use the **force-entry** statement to record all traffic from a suspect host, even traffic that would not otherwise be counted.

**ignore-entry** ensures that all IDS events are ignored. You can use this statement to disregard all traffic from a host you trust, including any temporary anomalies that IDS would otherwise count as events.

To configure an entry behavior different from the default, include the **force-entry** or **ignore-entry** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

```

[edit services ids rule rule-name term term-name then]
(force-entry | ignore-entry);

```

- **logging**—The event is logged in the system log file.

To configure logging, include the **logging** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

```

[edit services ids rule rule-name term term-name then]
logging {
  syslog;
  threshold rate;
}

```

You can optionally include a threshold rate to trigger the generation of system log messages. The threshold rate is specified in events per second. IDS logs are generated once every 60 seconds for each anomaly that is reported. The logs are generated as long as the events continue.

- **session-limit**—The router limits open sessions when the specified threshold is reached.

To configure a threshold, include the **session-limit** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

```

[edit services ids rule rule-name term term-name then]
session-limit {
  by-destination {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
  }
  by-pair {
    hold-time seconds;
    maximum number;
  }
}

```

```

        packets number;
        rate number;
    }
    by-source {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
    }
}

```

You configure the thresholds for flow limitation based on traffic direction:

- To limit the number of outgoing sessions from one internal host or subnet, configure the **by-source** statement.
- To limit the number of sessions between a pair of IP addresses, subnets, or applications, configure the **by-pair** statement.
- To limit the number of incoming sessions to one external public IP address or subnet, configure the **by-destination** statement.

For each direction, you can configure the following threshold values:

- **hold-time *seconds***—When the **rate** or **packets** measurement reaches the threshold value, stop all new flows for the specified number of seconds. Once **hold-time** is in effect, the traffic is blocked for the specified time even if the rate subsides below the specified limit. By default, **hold-time** has a value of 0; the range is 0 through 60 seconds.
- **maximum *number***—Maximum number of open sessions per IP address or subnet per application. The range is 1 through 32,767.
- **packets *number***—Maximum number of packets per second (pps) per IP address or subnet per application. The range is 4 through 2,147,483,647.
- **rate *number***—Maximum number of sessions per second per IP address or subnet per application. The range is 4 through 32,767.

If you include more than one source address in the match conditions configured at the **[edit services ids rule *rule-name* term *term-name* from]** hierarchy level, limits are applied for each source address independently. For example, the following configuration allows 20 connections from each source address (10.1.1.1 and 10.1.1.2), not 20 connections total. The same logic applies to the **applications** and **destination-address** match conditions.

```

[edit services ids rule rule-name term term-name]
  from {
    source-address 10.1.1.1;
    source-address 10.1.1.2;
  }
  then {
    session-limit by-source {
      maximum 20;
    }
  }
}

```



**NOTE:** IDS limits are applied to packets that are accepted by stateful firewall rules. They are not applied to packets discarded or rejected by stateful firewall rules. For example, if the stateful firewall accepts 75 percent of the incoming traffic and the remaining 25 percent is rejected or discarded, the IDS limit applies only to 75 percent of the traffic.

- **syn-cookie**—The router activates SYN-cookie defensive mechanisms.

To configure SYN-cookie values, include the **syn-cookie** statement at the **[edit services ids rule rule-name term term-name then]** hierarchy level:

```
[edit services ids rule rule-name term term-name then]
syn-cookie {
  mss value;
  threshold rate;
}
```

If you enable SYN-cookie defenses, you must include both a threshold rate to trigger SYN-cookie activity and a Transmission Control Protocol (TCP) maximum segment size (MSS) value for TCP delayed binding. The threshold rate is specified in SYN attacks per second. By default, the TCP MSS value is 1500; the range is from 128 through 8192.

**Related  
Documentation**

- [Configuring IDS Rule Sets on page 453](#)
- [Examples: Configuring IDS Rules on page 454](#)

## Configuring IDS Rule Sets

The **rule-set** statement defines a collection of IDS rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the **rule-set** statement at the **[edit services ids]** hierarchy level with a **rule** statement for each rule:

```
[edit services ids]
rule-set rule-set-name {
  rule rule-name;
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing continues to the next rule in the rule set. If none of the rules matches the packet, the packet is dropped by default.

**Related  
Documentation**

- [Configuring IDS Rules on page 447](#)
- [Examples: Configuring IDS Rules on page 454](#)

## Examples: Configuring IDS Rules

---

The following configuration adds a permanent entry to the IDS anomaly table when it encounters a flow with the destination address 10.410.6.2:

```
[edit services ids]
rule simple_ids {
  term 1 {
    from {
      destination-address 10.410.6.2/32;
    }
    then {
      force-entry;
      logging {
        threshold 1;
        syslog;
      }
    }
  }
  term default {
    then {
      aggregation {
        source-prefix 24;
      }
    }
  }
  match-direction input;
}
```

The IDS configuration works in conjunction with the stateful firewall mechanism and relies heavily on the anomalies reported by the stateful firewall. The following configuration example shows this relationship:

```
[edit services ids]
rule simple_ids {
  term 1 {
    from {
      source-address 10.30.20.2/32;
      destination-address {
        10.30.10.2/32;
        10.30.1.2/32 except;
      }
      applications appl-ftp;
    }
    then {
      force-entry;
      logging {
        threshold 5;
        syslog;
      }
      syn-cookie {
        threshold 10;
      }
    }
  }
}
```

```

    }
    match-direction input;
  }

```

The following example shows configuration of flow limits:

```

[edit services ids]
rule ids-all {
  match-direction input;
  term t1 {
    from {
      application-sets alg-set;
    }
    then {
      aggregation {
        destination-prefix 30; /* IDS action aggregation */
      }
      logging {
        threshold 10;
      }
      session-limit {
        by-destination {
          hold-time 0;
          maximum 10;
          packets 200;
          rate 100;
        }
        by-pair {
          hold-time 0;
          maximum 10;
          packets 200;
          rate 100;
        }
        by-source {
          hold-time 5;
          maximum 10;
          packets 200;
          rate 100;
        }
      }
    }
  }
}

```

- Related Documentation**
- [Configuring IDS Rules on page 447](#)
  - [Configuring IDS Rule Sets on page 453](#)



## CHAPTER 18

# Summary of Intrusion Detection Service Configuration Statements

The following sections explain each of the intrusion detection service (IDS) statements. The statements are organized alphabetically.

### aggregation

---

<b>Syntax</b>	<pre>aggregation {     destination-prefix <i>prefix-value</i>   destination-prefix-ipv6 <i>prefix-value</i>;     source-prefix <i>prefix-value</i>   source-prefix-ipv6 <i>prefix-value</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the type of data to be aggregated.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IDS Rules on page 447</a></li></ul>

## application-sets (Services IDS)

---

<b>Syntax</b>	<code>application-sets <i>set-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define one or more target application sets.
<b>Options</b>	<i>set-name</i> —Name of the target application set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li></ul>

## applications (Services IDS)

---

<b>Syntax</b>	<code>applications [ <i>application-names</i> ];</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define one or more applications to which IDS applies.
<b>Options</b>	<i>application-name</i> —Name of the target application.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li></ul>

## by-destination

---

Syntax	<pre>by-destination {     hold-time <i>seconds</i>;     maximum <i>number</i>;     packets <i>number</i>;     rate <i>number</i>; }</pre>
Hierarchy Level	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> <a href="#">session-limit</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply limit to sessions based on numbers generated from the configured destination (IP or subnet) or application.
Options	<p><b>hold-time <i>seconds</i></b>—Length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the <b>maximum</b>, <b>packets</b>, or <b>rate</b> statements.</p> <p><b>maximum <i>number</i></b>—Maximum number of open sessions per application or IP address.</p> <p><b>packets <i>number</i></b>—Maximum peak packets per second per application or IP address.</p> <p><b>rate <i>number</i></b>—Maximum number of sessions per second per application or IP address.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## by-pair

---

Syntax	<pre>by-pair {     hold-time <i>seconds</i>;     maximum <i>number</i>;     packets <i>number</i>;     rate <i>number</i>; }</pre>
Hierarchy Level	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> <a href="#">session-limit</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply limit to paired stateful firewall and NAT flows (forward and reverse).
Options	<p><b>hold-time <i>seconds</i></b>—Length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the <b>maximum</b>, <b>packets</b>, or <b>rate</b> statements.</p> <p><b>maximum <i>number</i></b>—Maximum number of open sessions per application or IP address.</p> <p><b>packets <i>number</i></b>—Maximum peak packets per second per application or IP address.</p> <p><b>rate <i>number</i></b>—Maximum number of sessions per second per application or IP address.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## by-source

---

Syntax	<pre>by-source {     hold-time <i>seconds</i>;     maximum <i>number</i>;     packets <i>number</i>;     rate <i>number</i>; }</pre>
Hierarchy Level	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> <a href="#">session-limit</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply limit to sessions based on numbers generated from the configured source (IP or subnet) or application.
Options	<p><b>hold-time <i>seconds</i></b>—Length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the <b>maximum</b>, <b>packets</b>, or <b>rate</b> statements.</p> <p><b>maximum <i>number</i></b>—Maximum number of open sessions per application or IP address.</p> <p><b>packets <i>number</i></b>—Maximum peak packets per second per application or IP address.</p> <p><b>rate <i>number</i></b>—Maximum number of sessions per second per application or IP address.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## destination-address (Services IDS)

---

Syntax	destination-address ( <i>address</i>   any-unicast) <except>;
Hierarchy Level	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
Release Information	Statement introduced before Junos OS Release 7.4. <i>address</i> option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
Description	Specify the destination address for rule matching.
Options	<i>address</i> —Destination IPv4 or IPv6 address or prefix value. <i>any-unicast</i> —Any unicast packet. <i>except</i> —(Optional) Exempt the specified address, prefix, or unicast packets from rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li></ul>

## destination-address-range (Services IDS)

---

Syntax	destination-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>;
Hierarchy Level	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
Release Information	Statement introduced in Junos OS Release 7.6. <i>minimum-value</i> and <i>maximum-value</i> options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
Description	Specify the destination address range for rule matching.
Options	<i>minimum-value</i> —Lower boundary for the IPv4 or IPv6 address range. <i>maximum-value</i> —Upper boundary for the IPv4 or IPv6 address range. <i>except</i> —(Optional) Exempt the specified address range from rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li></ul>

## destination-prefix (Services IDS)

---

<b>Syntax</b>	<code>destination-prefix <i>prefix-value</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> <a href="#">aggregation</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the prefix value for destination IPv4 address aggregation.
<b>Options</b>	<i>prefix-value</i> —Integer value. <b>Range:</b> 1 through 32
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## destination-prefix-ipv6

---

<b>Syntax</b>	<code>destination-prefix-ipv6 <i>prefix</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> <a href="#">aggregation</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Specify the prefix value for destination IPv6 address aggregation.
<b>Options</b>	<i>prefix-value</i> —Integer value. <b>Range:</b> 1 through 128
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## destination-prefix-list (Services IDS)

---

<b>Syntax</b>	<code>destination-prefix-list <i>list-name</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	<code>[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	Specify the destination prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the <code>[edit policy-options]</code> hierarchy level.
<b>Options</b>	<p><b>list-name</b>—Destination prefix list.</p> <p><b>except</b>—(Optional) Exclude the specified prefix list from rule matching.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Routing Policy Feature Guide for Routing Devices</i></li><li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li></ul>

## force-entry

---

<b>Syntax</b>	<code>(force-entry   ignore-entry);</code>
<b>Hierarchy Level</b>	<code>[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Specify handling of entries in the IDS events cache:</p> <ul style="list-style-type: none"><li>• <b>force-entry</b>—Ensure that the entry has a permanent place in the IDS cache after one event is registered.</li><li>• <b>ignore-entry</b>—Ensure that all IDS events are ignored.</li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## from (Services IDS)

---

<b>Syntax</b>	<pre> from {   application-sets set-name;   applications [ application-names ];   destination-address (address   any-unicast) &lt;except&gt;;   destination-address-range low minimum-value high maximum-value &lt;except&gt;;   source-address (address   any-unicast) &lt;except&gt;;   source-address-range low minimum-value high maximum-value &lt;except&gt;; } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> rule-name <a href="#">term</a> term-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify input conditions for the IDS term.
<b>Options</b>	<p>For information on match conditions, see the description of firewall filter match conditions in the <i>Routing Policy Feature Guide for Routing Devices</i>.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li> </ul>

## ignore-entry

---

See [force-entry](#)

## logging (Services IDS)

---

<b>Syntax</b>	<code>logging {     syslog;     threshold rate; }</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Set logging values for this IDS term.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## match-direction (Services IDS)

---

<b>Syntax</b>	<code>match-direction (input   output   input-output);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the direction in which the rule match is applied.
<b>Options</b>	<code>input</code> —Apply the rule match on input. <code>output</code> —Apply the rule match on output. <code>input-output</code> —Apply the rule match bidirectionally.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li></ul>

## mss

---

<b>Syntax</b>	<code>mss value;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> <a href="#">syn-cookie</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the maximum segment size (MSS) value used in Transmission Control Protocol (TCP) delayed binding.
<b>Options</b>	<b>value</b> —MSS value. <b>Default:</b> 1500 <b>Range:</b> 128 through 8192
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## rule (Services IDS)

```

Syntax  rule rule-name {
        match-direction (input | output | input-output);
        term term-name {
            from {
                application-sets set-name;
                applications [ application-names ];
                destination-address (address | any-unicast) <except>;
                destination-address-range low minimum-value high maximum-value <except>;
                source-address (address | any-unicast) <except>;
                source-address-range low minimum-value high maximum-value <except>;
            }
            then {
                aggregation {
                    destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
                    source-prefix prefix-value | source-prefix-ipv6 prefix-value;
                }
                (force-entry | ignore-entry);
                logging {
                    syslog;
                    threshold rate;
                }
                session-limit {
                    by-destination {
                        hold-time seconds;
                        maximum number;
                        packets number;
                        rate number;
                    }
                    by-pair {
                        hold-time seconds;
                        maximum number;
                        packets number;
                        rate number;
                    }
                    by-source {
                        hold-time seconds;
                        maximum number;
                        packets number;
                        rate number;
                    }
                }
                syn-cookie {
                    mss value;
                    threshold rate;
                }
            }
        }
    }

```

Hierarchy Level [edit [services](#) ids],  
 [edit [services](#) ids [rule-set](#) rule-set-name]

<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the rule the router uses when applying this service.
<b>Options</b>	<i>rule-name</i> —Identifier for the collection of terms that constitute this rule.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IDS Rules on page 447</a></li></ul>

---

## rule-set (Services IDS)

---

<b>Syntax</b>	<pre>rule-set rule-set-name {     [ rule rule-names ]; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<i>rule-set-name</i> —Identifier for the collection of rules that constitute this rule set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IDS Rule Sets on page 453</a></li></ul>

---

## services (IDS)

---

<b>Syntax</b>	<pre>services ids { ... }</pre>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the service rules to be applied to traffic.
<b>Options</b>	<i>ids</i> —Identifies the IDS set of rules statements.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IDS Rules on page 447</a></li></ul>

## session-limit

---

**Syntax**    session-limit {  
              by-destination {  
                  hold-time *seconds*;  
                  maximum *number*;  
                  packets *number*;  
                  rate *number*;  
              }  
              by-pair {  
                  hold-time *seconds*;  
                  maximum *number*;  
                  packets *number*;  
                  rate *number*;  
              }  
              by-source {  
                  hold-time *seconds*;  
                  maximum *number*;  
                  packets *number*;  
                  rate *number*;  
              }  
          }

**Hierarchy Level**    [edit [services](#) ids [rule](#) *rule-name* [term](#) *term-name* [then](#)]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Enable flow limitation by configuring thresholds on source, destination, or stateful firewall and network address translation (NAT) paired traffic flows.

**Options**    The remaining statements are described separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring Actions in IDS Rules on page 450](#)

## source-address (Services IDS)

<b>Syntax</b>	source-address ( <i>address</i>   any-unicast) <except>;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids rule <i>rule-name</i> term <i>term-name</i> from]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <i>address</i> option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Specify the source address for rule matching.
<b>Options</b>	<i>address</i> —Source IPv4 or IPv6 address or prefix value.  <i>any-unicast</i> —Any unicast packet.  <i>except</i> —(Optional) Exempt the specified address, prefix, or unicast packets from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li> </ul>

## source-address-range (Services IDS)

<b>Syntax</b>	source-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids rule <i>rule-name</i> term <i>term-name</i> from]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6. <i>minimum-value</i> and <i>maximum-value</i> options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Specify the source address range for rule matching.
<b>Options</b>	<i>minimum-value</i> —Lower boundary for the IPv4 or IPv6 address range.  <i>maximum-value</i> —Upper boundary for the IPv4 or IPv6 address range.  <i>except</i> —(Optional) Exempt the specified address range from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li> </ul>

## source-prefix (Services IDS)

---

<b>Syntax</b>	source-prefix <i>prefix-value</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> aggregation]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the prefix value for source IPv4 address aggregation.
<b>Options</b>	<i>prefix-value</i> —Integer value. <b>Range:</b> 1 through 32
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## source-prefix-ipv6

---

<b>Syntax</b>	source-prefix-ipv6 <i>prefix-value</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> aggregation]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Specify the prefix value for source IPv6 address aggregation.
<b>Options</b>	<i>prefix-value</i> —Integer value. <b>Range:</b> 1 through 128
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## source-prefix-list (Services IDS)

<b>Syntax</b>	source-prefix-list <i>list-name</i> <except>;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	Specify the source prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the [edit <b>policy-options</b> ] hierarchy level.
<b>Options</b>	<p><b>list-name</b>—Destination prefix list.</p> <p><b>except</b>—(Optional) Exclude the specified prefix list from rule matching.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Match Conditions in IDS Rules on page 449</a></li> <li>• <a href="#">Routing Policy Feature Guide for Routing Devices</a></li> </ul>

## syn-cookie

<b>Syntax</b>	<pre>syn-cookie {   <a href="#">mss</a> <i>value</i>;   <a href="#">threshold</a> <i>rate</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Enable SYN-cookie defenses against SYN attacks. By default, SYN-cookie techniques are not applied.
<b>Options</b>	The remaining statements are described separately.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li> </ul>

## syslog (Services IDS)

---

<b>Syntax</b>	syslog;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then logging</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Enable system logging. The system log information from the Adaptive Services or Multiservices Physical Interface Card (PIC) is passed to the kernel for logging in the <code>/var/log</code> directory.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

## term (Services IDS)

```
Syntax  term term-name {
        from {
            application-sets set-name;
            applications [ application-names ];
            destination-address (address | any-unicast) <except>;
            destination-address-range low minimum-value high maximum-value <except>;
            source-address (address | any-unicast) <except>;
            source-address-range low minimum-value high maximum-value <except>;
        }
        then {
            aggregation {
                destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
                source-prefix prefix-value | source-prefix-ipv6 prefix-value;
            }
            (force-entry | ignore-entry);
            logging {
                syslog;
                threshold rate;
            }
            session-limit {
                by-destination {
                    hold-time seconds;
                    maximum number;
                    packets number;
                    rate number;
                }
                by-pair {
                    hold-time seconds;
                    maximum number;
                    packets number;
                    rate number;
                }
                by-source {
                    hold-time seconds;
                    maximum number;
                    packets number;
                    rate number;
                }
            }
            syn-cookie {
                mss value;
                threshold rate;
            }
        }
    }
```

**Hierarchy Level** [edit [services](#) ids [rule](#) *rule-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the IDS term properties.

**Options**    *term-name*—Identifier for the term.

The remaining statements are explained separately.

**Required Privilege**    interface—To view this statement in the configuration.  
**Level**    interface-control—To add this statement to the configuration.

**Related**    • [Configuring IDS Rules on page 447](#)  
**Documentation**

## then (Services IDS)

```
Syntax  then {
        aggregation {
            destination-prefix prefix-number | destination-prefix-ipv6 prefix-value;
            source-prefix prefix-number | source-prefix-ipv6 prefix-value;
        }
        (force-entry | ignore-entry);
        logging {
            syslog;
            threshold rate;
        }
        session-limit {
            by-destination {
                hold-time seconds;
                maximum number;
                packets number;
                rate number;
            }
            by-pair {
                hold-time seconds;
                maximum number;
                packets number;
                rate number;
            }
            by-source {
                hold-time seconds;
                maximum number;
                packets number;
                rate number;
            }
        }
        syn-cookie {
            mss value;
            threshold rate;
        }
    }
```

**Hierarchy Level** [edit [services](#) ids [rule](#) *rule-name* [term](#) *term-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the IDS term actions.

**Options** The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring IDS Rules on page 447](#)

## threshold (Services)

---

<b>Syntax</b>	<code>threshold rate;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then logging</a> ], [edit <a href="#">services</a> ids <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then syn-cookie</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the threshold for logging or applying SYN-cookie defenses.
<b>Options</b>	<i>rate</i> —Logging threshold number of events per second.  <i>rate</i> —SYN-cookie defense number of SYN attacks per second.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in IDS Rules on page 450</a></li></ul>

# IPsec Services Configuration Guidelines

To configure IP Security (IPsec) services, include the following statements at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
clear-ike-sas-on-pic-restart;
clear-ipsec-sas-on-pic-restart;
ike {
  proposal proposal-name {
    authentication-algorithm (md5 | sha1 | sha-256);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group2 | group5 | group14);
    encryption-algorithm algorithm;
    lifetime-seconds seconds;
  }
  policy policy-name {
    description description;
    local-certificate identifier;
    local-id (ipv4_addr ipv4-address | ipv6_addr ipv6-address | key-id identifier);
    version (1 | 2);
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
    remote-id {
      any-remote-id;
      ipv4_addr [ values ];
      ipv6_addr [ values ];
      key_id [ values ];
    }
  }
}
ipsec {
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    description description;
    encryption-algorithm algorithm;
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
  }
  policy policy-name {
    description description;
    perfect-forward-secrecy {
```

```

        keys (group1 | group2);
    }
    proposals [ proposal-names ];
}
}
rule rule-name {
    match-direction (input | output);
    term term-name {
        from {
            destination-address address;
            ipsec-inside-interface interface-name;
            source-address address;
        }
        then {
            anti-replay-window-size bits;
            backup-remote-gateway address;
            clear-dont-fragment-bit;
            copy-dont-fragment-bit
            set-dont-fragment-bit
            dynamic {
                ike-policy policy-name;
                ipsec-policy policy-name;
            }
            initiate-dead-peer-detection;
            manual {
                direction (inbound | outbound | bidirectional) {
                    authentication {
                        algorithm (hmac-md5-96 | hmac-sha1-96);
                        key (ascii-text key | hexadecimal key);
                    }
                    auxiliary-spi spi-value;
                    encryption {
                        algorithm algorithm;
                        key (ascii-text key | hexadecimal key);
                    }
                    protocol (ah | bundle | esp);
                    spi spi-value;
                }
            }
            no-anti-replay;
            remote-gateway address;
            syslog;
            tunnel-mtu bytes;
        }
    }
}
}
rule-set rule-set-name {
    [ rule rule-names ];
}
no-ipsec-tunnel-in-traceroute;
traceoptions {
    file {
        files number;
        size bytes;
    }
    flag flag;
}

```

```

    level level;
}

```

This chapter includes the following sections:

- [Minimum Security Association Configurations on page 481](#)
- [Configuring Security Associations on page 483](#)
- [Configuring IKE Proposals on page 489](#)
- [Configuring IKE Policies on page 493](#)
- [Configuring IPsec Proposals on page 499](#)
- [Configuring IPsec Policies on page 501](#)
- [IPsec Policy for Dynamic Endpoints on page 504](#)
- [Configuring IPsec Rules on page 504](#)
- [Configuring IPsec Rule Sets on page 511](#)
- [Configuring Dynamic Endpoints for IPsec Tunnels on page 512](#)
- [Tracing IPsec Operations on page 517](#)
- [Configuring IPsec Using the Extension-Provider Package on page 519](#)
- [Examples: Configuring IPsec Services on page 520](#)

## Minimum Security Association Configurations

The following sections show the minimum configurations necessary to set up security associations (SAs) for IPsec services:

- [Minimum Manual SA Configuration on page 481](#)
- [Minimum Dynamic SA Configuration on page 482](#)

### Minimum Manual SA Configuration

To define a manual SA configuration, you must include at least the following statements at the `[edit services ipsec-vpn rule rule-name term term-name then manual]` hierarchy level:

```

[edit services ipsec-vpn rule rule-name term term-name then manual]
  direction (inbound | outbound | bidirectional) {
    authentication {
      algorithm (hmac-md5-96 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    encryption {
      algorithm algorithm;
      key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
  }

```

## Minimum Dynamic SA Configuration

To define a dynamic SA configuration, you must include at least the following statements at the `[edit services ipsec-vpn]` hierarchy level:

```
[edit services ipsec-vpn]
ike {
  proposal proposal-name {
    authentication-algorithm (md5 | sha1 | sha-256);
    authentication-method pre-shared-keys;
    dh-group (group1 | group2 | group5 | group14);
    encryption-algorithm algorithm;
  }
  policy policy-name {
    proposals [ ike-proposal-names ];
    pre-shared-key (ascii-text key | hexadecimal key);
    version (1 | 2);
    mode (aggressive | main);
  }
}
ipsec {
  policy policy-name {
    proposals [ ipsec-proposal-names ];
  }
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    encryption-algorithm algorithm;
    protocol (ah | esp | bundle);
  }
}
```



### NOTE:

- Starting with Junos OS Release 11.4, both IKEv1 and IKEv2 are supported by default on all M Series, MX Series, and T Series routers. The `version` statement at the `[edit services ipsec-vpn ike policy name]` hierarchy level allows you to configure the specific IKE version to be supported.
- The `mode` statement at the `[edit services ipsec-vpn ike policy name]` hierarchy level is required only if the `version` option is set to 1.

You must also include the `ipsec-policy` statement at the `[edit services ipsec-vpn rule rule-name term term-name then dynamic]` hierarchy level.

### Related Documentation

- [Understanding Junos VPN Site Secure on page 75](#)
- [Configuring Security Associations](#)
- [Configuring IKE Proposals](#)
- [Configuring IKE Policies](#)
- [Configuring IPsec Proposals](#)
- [Configuring IPsec Policies](#)

## Configuring Security Associations

To use Internet Protocol Security (IPsec) services, you create a Security Association (SA) between hosts.

This section includes the following topics:

- [Security Associations Overview on page 483](#)
- [Configuring Manual Security Associations on page 484](#)
- [Configuring Dynamic Security Associations on page 488](#)
- [Clearing Security Associations on page 489](#)



**NOTE:** Both OSPFv2 and OSPFv3 support IPsec authentication. However, dynamic or tunnel mode IPsec SAs are not supported for OSPFv3. If you add SAs into OSPFv3 by including the `ipsec-sa` statement at the `[edit protocols ospf3 area area-number interface interface-name]` hierarchy level, your configuration fails to commit. For more information about OSPF authentication and other OSPF properties, see the *Junos OS Routing Protocols Library for Routing Devices*.

## Security Associations Overview

A security association (SA) is set of security parameters that dictates how IPsec processes a packet. The SA defines what rules to use for authentication and encryption algorithms, key exchange mechanisms, and secure communications between two parties. A single secure tunnel uses multiple SAs. SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. You can configure two types of SAs:

- **Manual**—Requires no negotiation; all values, including the keys, are static and specified in the configuration. Manual SAs statically define the Security Parameter Index (SPI) values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. As a result, each peer must have the same configured options for communication to take place.

In IPsec, SPI is a numeric identifier, which is used with the destination address and security protocol to identify an SA. When IKE is used to establish an SA, the SPI is randomly derived. When manual configuration is used for an SA, the SPI must be entered as a parameter.

For information about how to configure a manual SA, see [“Configuring Manual Security Associations” on page 484](#).

- **Dynamic**—Specifies proposals to be negotiated with the tunnel peer. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. Dynamic SAs require additional configuration. The dynamic SA includes one or more **proposal** statements, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer. With dynamic SAs, you configure Internet

Exchange Key (IKE) first and then the SA. IKE is a part of IPsec that provides ways to exchange keys for encryption and authentication securely over an unsecured medium such as the Internet.

IKE employs Diffie-Hellman methods and is optional in IPsec (the shared keys can be entered manually at the endpoints). IKE creates dynamic security associations; it negotiates SAs for IPsec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway. This connection is then used to dynamically agree upon keys and other data used by the dynamic IPsec SA. The IKE SA is negotiated first and then used to protect the negotiations that determine the dynamic IPsec SAs. IKE enables a pair of security gateways to:

- Dynamically establish a secure tunnel over which security gateways can exchange tunnel and key information.
- Set up user-level tunnels or SAs, including tunnel attribute negotiations and key management. These tunnels can also be refreshed and terminated on top of the same secure channel.

For information about how to configure a dynamic SA, see [“Configuring Dynamic Security Associations” on page 488](#).

For more information on Security Associations, see *Security Associations Overview*

## Configuring Manual Security Associations

Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place.

To configure a manual IPsec security association, include statements at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
direction (inbound | outbound | bidirectional) {
  authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
  }
  auxiliary-spi auxiliary-spi-value;
  encryption {
    algorithm algorithm;
    key (ascii-text key | hexadecimal key);
  }
  protocol (ah | esp | bundle);
  spi spi-value;
}
```

To configure manual SA statements, do the following:

- [Configuring the Direction for IPsec Processing on page 485](#)
- [Configuring the Protocol for a Manual IPsec SA on page 486](#)
- [Configuring the Security Parameter Index on page 486](#)
- [Configuring the Auxiliary Security Parameter Index on page 486](#)

- [Configuring Authentication for a Manual IPsec SA on page 486](#)
- [Configuring Encryption for a Manual IPsec SA on page 487](#)

### Configuring the Direction for IPsec Processing

The **direction** statement specifies inbound or outbound IPsec processing. If you want to define different algorithms, keys, or security parameter index (SPI) values for each direction, you configure the **inbound** and **outbound** options. If you want the same attributes in both directions, use the **bidirectional** option.

To configure the direction of IPsec processing, include the **direction** statement at the **[edit services ipsec-vpn rule rule-name term term-name then manual]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
  direction (inbound | outbound | bidirectional) {
  ...
}
```

#### *Example: Using Different Configuration for the Inbound and Outbound Directions*

Define different algorithms, keys, and security parameter index values for each direction:

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
  direction inbound {
    protocol esp;
    spi 16384;
    encryption {
      algorithm 3des-cbc;
      key ascii-text 23456789012345678901234;
    }
  }
  direction outbound {
    protocol esp;
    spi 24576;
    encryption {
      algorithm 3des-cbc;
      key ascii-text 12345678901234567890abcd;
    }
  }
```

#### *Example: Using the Same Configuration for the Inbound and Outbound Directions*

Define one set of algorithms, keys, and security parameter index values that is valid in both directions:

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
  direction bidirectional {
    protocol ah;
    spi 20001;
    authentication {
      algorithm hmac-md5-96;
      key ascii-text 123456789012abcd;
    }
  }
```

### Configuring the Protocol for a Manual IPsec SA

---

IPsec uses two protocols to protect IP traffic: Encapsulating Security Payload (ESP) and authentication header (AH). The AH protocol is used for strong authentication. A third option, **bundle**, uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.

To configure the IPsec protocol, include the **protocol** statement and specify the **ah**, **esp**, or **bundle** option at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual direction *direction*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
  protocol (ah | bundle | esp);
```

### Configuring the Security Parameter Index

---

An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets.



**NOTE:** Each manual SA must have a unique SPI and protocol combination. Use the auxiliary SPI when you configure the **protocol** statement to use the **bundle** option.

To configure the SPI, include the **spi** statement and specify a value (from 256 through 16,639) at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual direction *direction*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
  spi spi-value;
```

### Configuring the Auxiliary Security Parameter Index

---

Use the auxiliary SPI when you configure the **protocol** statement to use the **bundle** option.



**NOTE:** Each manual SA must have a unique SPI and protocol combination.

To configure the auxiliary SPI, include the **auxiliary-spi** statement and specify a value (from 256 through 16,639) at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual direction *direction*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
  auxiliary-spi auxiliary-spi-value;
```

### Configuring Authentication for a Manual IPsec SA

---

To configure an authentication algorithm, include the **authentication** statement and specify an authentication algorithm and a key at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual direction *direction*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
  authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
  }
```

The algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit authenticator value and a 96-bit digest.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit authenticator value and a 96-bit digest.

The key can be one of the following:

- **ascii-text**—ASCII text key. With the **hmac-md5-96** option, the key contains 16 ASCII characters. With the **hmac-sha1-96** option, the key contains 20 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the **hmac-md5-96** option, the key contains 32 hexadecimal characters. With the **hmac-sha1-96** option, the key contains 40 hexadecimal characters.

### Configuring Encryption for a Manual IPsec SA

To configure IPsec encryption, include the **encryption** statement and specify an algorithm and key at the **[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
  encryption {
    algorithm algorithm;
    key (ascii-text key | hexadecimal key);
  }
```

The algorithm can be one of the following:

- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 64 bits long.
- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.



**NOTE:** For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409, *The Internet Key Exchange (IKE)*. The AES encryption algorithms use a software implementation that has much lower throughput, so DES remains the recommended option. For reference information on AES encryption, see RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

For **3des-cbc**, the first 8 bytes should differ from the second 8 bytes, and the second 8 bytes should be the same as the third 8 bytes.

If you configure an authentication proposal but do not include the encryption statement, the result is NULL encryption. Certain applications expect this result. If you configure no specific authentication or encryption values, the Junos OS uses the default values of **sha1** for the authentication and **3des-cbc** for the encryption.

---

The key can be one of the following:

- **ascii-text**—ASCII text key. With the **des-cbc** option, the key contains 8 ASCII characters. With the **3des-cbc** option, the key contains 24 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the **des-cbc** option, the key contains 16 hexadecimal characters. With the **3des-cbc** option, the key contains 48 hexadecimal characters.



**NOTE:** You cannot configure encryption when you use the AH protocol.

---

## Configuring Dynamic Security Associations

You configure dynamic SAs with a set of proposals that are negotiated by the security gateways. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more proposals, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer.

To enable a dynamic SA, follow these steps:

1. Configure Internet Key Exchange (IKE) proposals and IKE policies associated with these proposals.
2. Configure IPsec proposals and an IPsec policy associated with these proposals.
3. Associate an SA with an IPsec policy by configuring the **dynamic** statement.

For more information about IKE policies and proposals, see [“Configuring IKE Policies” on page 493](#) and [“Configuring IKE Proposals” on page 489](#). For more information about IPsec policies and proposals, see [“Configuring IPsec Policies” on page 501](#).

To configure a dynamic SA, include the **dynamic** statement and specify an IPsec policy name at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level. The **ike-policy** statement is optional unless you use the preshared key authentication method.

```
[edit services ipsec-vpn rule rule-name term term-name then]
dynamic {
  ike-policy policy-name;
  ipsec-policy policy-name;
}
```



**NOTE:** If you want to establish a dynamic SA, the attributes in at least one configured IPsec and IKE proposal must match those of its peer.

## Clearing Security Associations

You can set up the router software to clear IKE or IPsec SAs automatically when the corresponding services PIC restarts or is taken offline. To configure this property, include the **clear-ike-sas-on-pic-restart** or **clear-ipsec-sas-on-pic-restart** statement at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
clear-ike-sas-on-pic-restart;
clear-ipsec-sas-on-pic-restart;
```

After you add this statement to the configuration, all the IKE or IPsec SAs corresponding to the tunnels in the PIC will be cleared when the PIC restarts or goes offline.

### Related Documentation

- *IKE Key Management Protocol Overview*
- *IPsec Requirements for Junos-FIPS*
- *Security Services Configuration Statements*

## Configuring IKE Proposals

Dynamic security associations (SAs) require IKE configuration. With dynamic SAs, you configure IKE first, and then the SA. IKE creates the dynamic SAs and negotiates them for IPsec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway.

You can configure one or more IKE proposals. Each proposal is a list of IKE attributes to protect the IKE connection between the IKE host and its peer.



**NOTE:** In IKEv1, the authentication method for SAs is negotiated with the remote peer based on the type of authentication method configured in the IKE proposal. In IKEv2, such a negotiation is not performed with the remote peer. Instead, each IKE peer uses the authentication method that is locally configured for them.

For SAs in IKEv2, the authentication method is either the default value as IKEv1 (if another authentication method is not configured in the IKE proposal) or all IKEv2 proposals in the IKE policy must be configured with the same authentication method value.

To configure an IKE proposal, include the **proposal** statement and specify a name at the **[edit services ipsec-vpn ike]** hierarchy level:

```
[edit services ipsec-vpn ike]
proposal proposal-name {
  authentication-algorithm (md5 | sha1 | sha-256);
  authentication-method (dsa-signatures | pre-shared-key | rsa-signatures);
  dh-group (group1 | group2 | group5 | group14);
  encryption-algorithm algorithm;
  lifetime-seconds seconds;
}
```

This section includes the following topics:

- [Configuring the Authentication Algorithm for an IKE Proposal on page 490](#)
- [Configuring the Authentication Method for an IKE Proposal on page 491](#)
- [Configuring the Diffie-Hellman Group for an IKE Proposal on page 491](#)
- [Configuring the Encryption Algorithm for an IKE Proposal on page 492](#)
- [Configuring the Lifetime for an IKE SA on page 492](#)
- [Example: Configuring an IKE Proposal on page 493](#)

## Configuring the Authentication Algorithm for an IKE Proposal

To configure the authentication algorithm for an IKE proposal, include the **authentication-algorithm** statement at the **[edit services ipsec-vpn ike proposal proposal-name]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]
authentication-algorithm (md5 | sha1 | sha-256);
```

The authentication algorithm can be one of the following:

- **md5**—Produces a 128-bit digest.
- **sha1**—Produces a 160-bit digest.
- **sha-256**—Produces a 256-bit digest.



**NOTE:** For reference information on Secure Hash Algorithms (SHAs), see Internet draft draft-eastlake-sha2-02.txt, *Secure Hash Algorithms (SHA and HMAC-SHA)* (expires July 2006).

## Configuring the Authentication Method for an IKE Proposal

To configure the authentication method for an IKE proposal, include the **authentication-method** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]  
authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
```

The authentication method can be one of the following:

- **dsa-signatures**—Digital Signature Algorithm
- **pre-shared-keys**—A key derived from an out-of-band mechanism; the key authenticates the exchanges
- **rsa-signatures**—Public key algorithm (supports encryption and digital signatures)

## Configuring the Diffie-Hellman Group for an IKE Proposal

Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel. It is also used within IKE to establish session keys.

To configure the Diffie-Hellman group for an IKE proposal, include the **dh-group** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]  
dh-group (group1 | group2 | group5 | group14);
```

The group can be one of the following:

- **group1**—Specifies that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group2**—Specifies that IKE use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group5**—Specifies that IKE use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group14**—Specifies that IKE use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

Using a Diffie-Hellman group based on a greater number of bits results a more secure IKE tunnel than using a group based on fewer bits. However, this additional security entails additional processing time.

## Configuring the Encryption Algorithm for an IKE Proposal

To configure the encryption algorithm for an IKE proposal, include the **encryption-algorithm** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]  
  encryption-algorithm algorithm;
```

The encryption algorithm can be one of the following:

- **3des-cbc**—Cipher block chaining encryption algorithm with a key size of 24 bytes; its key size is 192 bits long.
- **des-cbc**—Cipher block chaining encryption algorithm with a key size of 8 bytes; its key size is 56 bits long.
- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.



**NOTE:** For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409, *The Internet Key Exchange (IKE)*. The AES encryption algorithms use a software implementation that has much lower throughput, so DES remains the recommended option.

For 3des-cbc, the first 8 bytes should differ from the second 8 bytes, and the second 8 bytes should be the same as the third 8 bytes.

If you configure an authentication proposal but do not include the encryption statement, the result is NULL encryption. Certain applications expect this result. If you configure no specific authentication or encryption values, the Junos OS uses the default values of sha1 for the authentication and 3des-cbc for the encryption.

---

## Configuring the Lifetime for an IKE SA

The **lifetime-seconds** statement sets the lifetime of an IKE SA. When the IKE SA expires, it is replaced by a new SA (and SPI) or the IPsec connection is terminated.

To configure the lifetime for an IKE SA, include the **lifetime-seconds** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]  
  lifetime-seconds seconds;
```

By default, the IKE SA lifetime is 3600 seconds. The range is from 180 through 86,400 seconds.



**NOTE:** In IKEv1, the lifetime for SAs is negotiated with the remote peer based on the type of lifetime configured in the IKE proposal. In IKEv2, such a negotiation is not performed with the remote peer. Instead, each IKE peer uses the lifetime that is locally configured for them.

For SAs in IKEv2, the lifetime is either the default value as IKEv1 (if another lifetime is not configured in the IKE proposal) or all IKEv2 proposals in the IKE policy must be configured with the same lifetime value.



**NOTE:** For IKE proposals, there is only one SA lifetime value, specified by the Junos OS. IPsec proposals use a different mechanism; for more information, see [“Configuring the Lifetime for an IPsec SA” on page 500](#).

### Example: Configuring an IKE Proposal

Configure an IKE proposal:

```
[edit services ipsec-vpn ike]
proposal ike-proposal {
  authentication-method pre-shared-keys;
  dh-group group1;
  authentication-algorithm sha1;
  encryption-algorithm 3des-cbc;
}
```

### Configuring IKE Policies

An IKE policy defines a combination of security parameters (IKE proposals) to be used during IKE negotiation. It defines a peer address and the proposals needed for that connection. Depending on which authentication method is used, it defines the preshared key for the given peer or the local certificate. During the IKE negotiation, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used. The configured preshared key must also match its peer.

Starting with Junos OS Release 11.4, both IKEv1 and IKEv2 are supported by default on all M Series, MX Series, and T Series routers. You can configure the specific IKE phase to be supported for the negotiation. However, if only IKEv1 is supported, the Junos OS rejects IKEv2 negotiations. Similarly, if only IKEv2 is supported, the Junos OS rejects all IKEv1 negotiations.

The key management process (kmd) daemon determines which version of IKE is used in a negotiation. If kmd is the IKE initiator, it uses IKEv1 by default and retains the configured

version for negotiations. If `kmd` is the IKE responder, it accepts connections from both IKEv1 and IKEv2.

You can create multiple, prioritized proposals at each peer to ensure that at least one proposal matches a remote peer's proposal.

First, you configure one or more IKE proposals; then you associate these proposals with an IKE policy. You can also prioritize a list of proposals used by IKE in the **policy** statement by listing the proposals you want to use, from first to last.

To configure an IKE policy, include the **policy** statement and specify a policy name at the **[edit services ipsec-vpn ike]** hierarchy level:

```
[edit services ipsec-vpn ike]
policy policy-name {
  description description;
  local-certificate identifier;
  local-id (ipv4_addr ipv4-address | ipv6_addr ipv6-address | key-id identifier);
  version (1 | 2);
  mode (aggressive | main);
  pre-shared-key (ascii-text key | hexadecimal key);
  proposals [ proposal-names ];
  remote-id {
    any-remote-id;
    ipv4_addr [ values ];
    ipv6_addr [ values ];
    key_id [ values ];
  }
}
```

This section includes the following topics:

- [Configuring the IKE Phase on page 494](#)
- [Configuring the Mode for an IKE Policy on page 495](#)
- [Configuring the Proposals in an IKE Policy on page 495](#)
- [Configuring the Preshared Key for an IKE Policy on page 495](#)
- [Configuring the Local Certificate for an IKE Policy on page 496](#)
- [Configuring the Description for an IKE Policy on page 497](#)
- [Configuring Local and Remote IDs for IKE Phase 1 Negotiation on page 497](#)
- [Example: Configuring an IKE Policy on page 498](#)

For an example of an IKE policy configuration, see “[Example: Configuring an IKE Policy](#)” on page 498.

## Configuring the IKE Phase

Starting with Junos OS Release 11.4, both IKEv1 and IKEv2 are supported by default on all M Series, MX Series, and T Series routers. You can configure the specific IKE phase to be supported for the negotiation. However, if only IKEv1 is supported, the Junos OS rejects IKEv2 negotiations. Similarly, if only IKEv2 is supported, the Junos OS rejects all IKEv1 negotiations.

To configure the IKE phase used, include the **version** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]  
version (1 | 2);
```

## Configuring the Mode for an IKE Policy

IKE policy has two modes: aggressive and main. By default, main mode is enabled. Main mode uses six messages, in three exchanges, to establish the IKE SA. (These three steps are IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer.) Main mode also allows a peer to hide its identity.

Aggressive mode also establishes an authenticated IKE SA and keys. However, aggressive mode uses half the number of messages, has less negotiation power, and does not provide identity protection. The peer can use the aggressive or main mode to start IKE negotiation; the remote peer accepts the mode sent by the peer.



**NOTE:** The mode configuration is required only if the version option is set to 1.

To configure the mode for an IKE policy, include the **mode** statement and specify **aggressive** or **main** at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]  
mode (aggressive | main);
```

## Configuring the Proposals in an IKE Policy

The IKE policy includes a list of one or more proposals associated with an IKE policy.

To configure the proposals in an IKE policy, include the **proposals** statement and specify one or more proposal names at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
proposals [ proposal-names ];
```

## Configuring the Preshared Key for an IKE Policy

When you include the **authentication-method pre-shared-keys** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level, IKE policy preshared keys authenticate peers; for more information, see [“Configuring the Authentication Method for an IKE Proposal” on page 491](#). You must manually configure a preshared key, which must match that of its peer. The preshared key can be an ASCII text (alphanumeric) key or a hexadecimal key.

To configure the preshared key in an IKE policy, include the **pre-shared-key** statement and a key at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]  
pre-shared-key (ascii-text key | hexadecimal key);
```

The key can be one of the following:

- **ascii-text**—ASCII text key. With the **des-cbc** option, the key contains 8 ASCII characters. With the **3des-cbc** option, the key contains 24 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the **des-cbc** option, the key contains 16 hexadecimal characters. With the **3des-cbc** option, the key contains 48 hexadecimal characters.

## Configuring the Local Certificate for an IKE Policy

When you include the **authentication-method rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level, public key infrastructure (PKI) digital certificates authenticate peers; for more information, see [“Configuring the Authentication Method for an IKE Proposal” on page 491](#). You must identify a local certificate that is sent to the peer during the IKE authentication phase.

To configure the local certificate for an IKE policy, include the **local-certificate** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]  
  local-certificate identifier;
```

The **local-certificate** statement specifies the identifier used to obtain the end entity's certificate from the certification authority. Configuring it in an IKE policy allows you the flexibility of using a separate certificate with each remote peer if that is needed. You must also specify the identity of the certification authority by configuring the **ca-profile** statement at the **[edit security pki]** hierarchy level; for more information, see the *Junos OS Administration Library for Routing Devices*. For complete examples of digital certificate configuration, see the *Junos OS, Release 14.1*.

You can use the configured profiles to establish a set of trusted certification authorities for use with a particular service set. This enables you to configure separate service sets for individual clients to whom you are providing IP services; the distinct service sets provide logical separation of one set of IKE sessions from another, using different local gateway addresses, or *virtualization*. To configure the set of trusted certification authorities, include the **trusted-ca** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level:

```
[edit services service-set service-set-name ipsec-vpn-options]  
  trusted-ca ca-profile;
```

For more information, see [“Configuring IPsec Service Sets” on page 748](#).

---

## Configuring a Certificate Revocation List

A certificate revocation list (CRL) contains a list of digital certificates that have been cancelled before their expiration date. When a participating peer uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL.



**NOTE:** By default, certificate revocation list verification is enabled. You can disable CRL verification by including the `disable` statement at the `[edit security pki ca-profile ca-profile-name revocation-check]` hierarchy level.

By default, if the router either cannot access the Lightweight Directory Access Protocol (LDAP) URL or retrieve a valid certificate revocation list, certificate verification fails and the IPsec tunnel is not established. To override this behavior and permit the authentication of the IPsec peer when the CRL is not downloaded, include the `disable on-download-failure` statement at the `[edit security pki ca-profile ca-profile-name revocation-check crl]` hierarchy level.

To use the CA certificate revocation list, you include statements at the `[edit security pki ca-profile ca-profile-name revocation-check]` hierarchy level. For details, see the *Junos OS Administration Library for Routing Devices*.

## Configuring the Description for an IKE Policy

To specify an optional text description for an IKE policy, include the `description` statement at the `[edit services ipsec-vpn ike policy policy-name]` hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
description description;
```

## Configuring Local and Remote IDs for IKE Phase 1 Negotiation

You can optionally specify local identifiers for use in IKE phase 1 negotiation. If the `local-id` statement is omitted, the local gateway address is used.

To specify one or more local IDs, include the `local-id` statement at the `[edit services ipsec-vpn ike policy policy-name]` hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
local-id (ipv4_addr ipv4-address | ipv6_addr ipv6-address | key-id identifier);
```

You can also specify remote gateway identifiers for which the IKE policy is used. The remote gateway address in which this policy is defined is added by default.

To specify one or more remote IDs, include the `remote-id` statement at the `[edit services ipsec-vpn ike policy policy-name]` hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
remote-id {
  any-remote-id;
  ipv4_addr [ values ];
  ipv6_addr [ values ];
  key_id [ values ];
}
```

The `any-remote-id` option allows any remote address to connect. You must configure the `any-remote-id` option only with dynamic endpoints. If you configure this option with static endpoints, an error message is displayed stating that you can configure any remote

address only with dynamic endpoints. For more information about dynamic endpoint configurations, see [“Configuring Dynamic Endpoints for IPsec Tunnels”](#) on page 512.

### Example: Configuring an IKE Policy

Define two IKE policies: **policy 10.1.1.2** and **policy 10.1.1.1**. Each policy is associated with **proposal-1** and **proposal-2**. The following configuration uses only IKEv1 for negotiation.

```
[edit services ipsec-vpn]
ike {
  proposal proposal-1 {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 1000;
  }
  proposal proposal-2 {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
    lifetime-seconds 10000;
  }
  proposal proposal-3 {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
    lifetime-seconds 10000;
  }
  policy 10.1.1.2 {
    mode main;
    proposals [ proposal-1 proposal-2 ];
    pre-shared-key ascii-text example-pre-shared-key;
  }
  policy 10.1.1.1 {
    local-certificate certificate-file-name;
    local-key-pair private-public-key-file;
    mode aggressive;
    proposals [ proposal-2 proposal-3 ]
    pre-shared-key hexadecimal 0102030abbcdd;
  }
}
```



**NOTE:** Updates to the current IKE proposal and policy configuration are not applied to the current IKE SA; updates are applied to new IKE SAs.

If you want the new updates to take immediate effect, you must clear the existing IKE security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IKE security association, see the [CLI Explorer](#).

---

## Configuring IPsec Proposals

An IPsec proposal lists protocols and algorithms (security services) to be negotiated with the remote IPsec peer.

To configure an IPsec proposal, include the **proposal** statement and specify an IPsec proposal name at the **[edit services ipsec-vpn ipsec]** hierarchy level:

```
[edit services ipsec-vpn ipsec]
proposal proposal-name {
  authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
  description description;
  encryption-algorithm algorithm;
  lifetime-seconds seconds;
  protocol (ah | esp | bundle);
}
```

This section discusses the following topics:

- [Configuring the Authentication Algorithm for an IPsec Proposal on page 499](#)
- [Configuring the Description for an IPsec Proposal on page 499](#)
- [Configuring the Encryption Algorithm for an IPsec Proposal on page 500](#)
- [Configuring the Lifetime for an IPsec SA on page 500](#)
- [Configuring the Protocol for a Dynamic SA on page 501](#)

### Configuring the Authentication Algorithm for an IPsec Proposal

To configure the authentication algorithm for an IPsec proposal, include the **authentication-algorithm** statement at the **[edit services ipsec-vpn ipsec proposal proposal-name]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]
authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
```

The authentication algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit digest. Only 96 bits are used for authentication.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit digest. Only 96 bits are used for authentication.

### Configuring the Description for an IPsec Proposal

To specify an optional text description for an IPsec proposal, include the **description** statement at the **[edit services ipsec-vpn ipsec proposal proposal-name]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]
description description;
```

## Configuring the Encryption Algorithm for an IPsec Proposal

To configure encryption algorithm for an IPsec proposal, include the **encryption-algorithm** statement at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]  
  encryption-algorithm algorithm;
```

The encryption algorithm can be one of the following:

- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 48 bits long.
- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.



**NOTE:** For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409, *The Internet Key Exchange (IKE)*. The AES encryption algorithms use a software implementation that has much lower throughput, so DES remains the recommended option.

For 3des-cbc, the first 8 bytes should differ from the second 8 bytes, and the second 8 bytes should be the same as the third 8 bytes.

If you configure an authentication proposal but do not include the encryption statement, the result is NULL encryption. Certain applications expect this result. If you configure no specific authentication or encryption values, the Junos OS uses the default values of sha1 for the authentication and 3des-cbc for the encryption.

---

## Configuring the Lifetime for an IPsec SA

When a dynamic IPsec SA is created, two types of lifetimes are used: hard and soft. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires.



**NOTE:** In IKEv1, the lifetime for SAs is negotiated with the remote peer based on the type of lifetime configured in the IPsec proposal. In IKEv2, such a negotiation is not performed with the remote peer. Instead, each IKE peer uses the lifetime that is locally configured for them.

For SAs in IKEv2, the lifetime is either the default value as IKEv1 (if another lifetime is not configured in the IPsec proposal) or all IKEv2 proposals in the IPsec policy must be configured with the same lifetime value.

To configure the hard lifetime value, include the **lifetime-seconds** statement and specify the number of seconds at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]
lifetime-seconds seconds;
```

The default lifetime is 28,800 seconds. The range is from 180 through 86,400 seconds.

The soft lifetime values are as follows:

- Initiator: Soft lifetime = Hard lifetime – 135 seconds.
- Responder: Soft lifetime = Hard lifetime – 90 seconds.

## Configuring the Protocol for a Dynamic SA

The **protocol** statement sets the protocol for a dynamic SA. IPsec uses two protocols to protect IP traffic: ESP and AH. The ESP protocol can support authentication, encryption, or both. The AH protocol is used for strong authentication. AH also authenticates the IP packet. The **bundle** option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.

To configure the protocol for a dynamic SA, include the **protocol** statement and specify the **ah**, **esp**, or **bundle** option at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]
protocol (ah | esp | bundle);
```

## Configuring IPsec Policies

An IPsec policy defines a combination of security parameters (IPsec proposals) used during IPsec negotiation. It defines Perfect Forward Secrecy (PFS) and the proposals needed for the connection. During the IPsec negotiation, IPsec looks for a proposal that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used.

You can create multiple, prioritized IPsec proposals at each peer to ensure that at least one proposal matches a remote peer's proposal.

First, you configure one or more IPsec proposals; then you associate these proposals with an IPsec policy. You can prioritize a list of proposals used by IPsec in the **policy** statement by listing the proposals you want to use, from first to last.

To configure an IPsec policy, include the **policy** statement, and specify the policy name and one or more proposals to associate with the policy, at the **[edit services ipsec-vpn ipsec]** hierarchy level:

```
[edit services ipsec-vpn ipsec]
policy policy-name {
  description description;
  perfect-forward-secrecy {
    keys (group1 | group2 | group5 | group14);
  }
  proposals [ proposal-names ];
}
```

This section includes the following topics related to configuring an IPsec policy:

- [Configuring the Description for an IPsec Policy on page 502](#)
- [Configuring Perfect Forward Secrecy on page 502](#)
- [Configuring the Proposals in an IPsec Policy on page 503](#)
- [Example: Configuring an IPsec Policy on page 503](#)

## Configuring the Description for an IPsec Policy

To specify an optional text description for an IPsec policy, include the **description** statement at the **[edit services ipsec-vpn ipsec policy policy-name]** hierarchy level:

```
[edit services ipsec-vpn ipsec policy policy-name]
description description;
```

## Configuring Perfect Forward Secrecy

PFS provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys. This statement is optional.

To configure PFS, include the **perfect-forward-secrecy** statement and specify a Diffie-Hellman group at the **[edit services ipsec-vpn ipsec policy policy-name]** hierarchy level:

```
[edit services ipsec-vpn ipsec policy policy-name]
perfect-forward-secrecy {
  keys (group1 | group2 | group5 | group14);
}
```

The key can be one of the following:

- **group1**—Specifies that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group2**—Specifies that IKE use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group5**—Specifies that IKE use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group14**—Specifies that IKE use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

The higher numbered groups provide more security than the lowered numbered groups,, but require more processing time.

## Configuring the Proposals in an IPsec Policy

The IPsec policy includes a list of one or more proposals associated with an IPsec policy.

To configure the proposals in an IPsec policy, include the **proposals** statement and specify one or more proposal names at the **[edit services ipsec-vpn ipsec policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec policy policy-name]  
proposals [ proposal-names ];
```

## Example: Configuring an IPsec Policy

Define an IPsec policy, **dynamic policy-1**, that is associated with two proposals (**dynamic-1** and **dynamic-2**):

```
[edit services ipsec-vpn ipsec]  
proposal dynamic-1 {  
  protocol esp;  
  authentication-algorithm hmac-md5-96;  
  encryption-algorithm 3des-cbc;  
  lifetime-seconds 6000;  
}  
proposal dynamic-2 {  
  protocol esp;  
  authentication-algorithm hmac-sha1-96;  
  encryption-algorithm 3des-cbc;  
  lifetime-seconds 6000;  
}  
policy dynamic-policy-1 {  
  perfect-forward-secrecy {  
    keys group1;  
  }  
  proposals [ dynamic-1 dynamic-2 ];  
}
```



**NOTE:** Updates to the current IPsec proposal and policy configuration are not applied to the current IPsec SA; updates are applied to new IPsec SAs.

If you want the new updates to take immediate effect, you must clear the existing IPsec security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IPsec security association, see the [CLI Explorer](#).

---

## IPsec Policy for Dynamic Endpoints

An IPsec policy for dynamic endpoints defines a combination of security parameters (IPsec proposals) used during IPsec negotiation between dynamic peer security gateways, in which the remote ends of tunnels do not have a statically assigned IP address.

During the IPsec negotiation, the IPsec policy looks for an IPsec proposal that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match. A match is made when the policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used.

If no policy is set, any policy proposed by the dynamic peer is accepted.

For more information about configuring IPsec policy, see “[Configuring IPsec Policies](#)” on [page 501](#).

**Related Documentation**

- [Configuring IPsec Policies on page 501](#)

---

## Configuring IPsec Rules

To configure an IPsec rule, include the **rule** statement and specify a rule name at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      destination-address address;
      ipsec-inside-interface interface-name;
      source-address address;
    }
    then {
      anti-replay-window-size bits;
      backup-remote-gateway address;
      clear-dont-fragment-bit;
      copy-dont-fragment-bit;
      set-dont-fragment-bit;
      dynamic {
```

```

    ike-policy policy-name;
    ipsec-policy policy-name;
  }
  initiate-dead-peer-detection;
  manual {
    direction (inbound | outbound | bidirectional) {
      authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      auxiliary-spi spi-value;
      encryption {
        algorithm algorithm;
        key (ascii-text key | hexadecimal key);
      }
      protocol (ah | bundle | esp);
      spi spi-value;
    }
  }
  no-anti-replay;
  remote-gateway address;
  syslog;
  tunnel-mtu bytes;
}

```

Each IPsec rule consists of a set of terms, similar to a firewall filter. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software.

The following sections explain how to configure the components of IPsec rules:

- [Configuring Match Direction for IPsec Rules on page 505](#)
- [Configuring Match Conditions in IPsec Rules on page 506](#)
- [Configuring Actions in IPsec Rules on page 508](#)

## Configuring Match Direction for IPsec Rules

Each rule must include a **match-direction** statement that specifies whether the match is applied on the input or output side of the interface. To configure where the match is applied, include the **match-direction (input | output)** statement at the **[edit services ipsec-vpn rule *rule-name*]** hierarchy level:

```

[edit services ipsec-vpn rule rule-name]
  match-direction (input | output);

```

The match direction is used with respect to the traffic flow through the AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.

With a next-hop service set, packet direction is determined by the interface used to route the packet to the AS or Multiservices PIC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the PIC, the packet direction is output. For more information on inside and outside interfaces, see [“Configuring Service Sets to be Applied to Services Interfaces” on page 742](#).

On the AS or Multiservices PIC, a flow lookup is performed. If no flow is found, rule processing is performed. All rules in the service set are considered. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that match the packet direction are considered.

## Configuring Match Conditions in IPsec Rules

To configure the match conditions in an IPsec rule, include the **from** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name]  
from {  
  destination-address address;  
  ipsec-inside-interface interface-name;  
  source-address address;  
}
```

You can use either the source address or the destination address as a match condition, in the same way that you would configure a firewall filter; for more information, see the *Routing Policy Feature Guide for Routing Devices*.

IPsec services support both IPv4 and IPv6 address formats. If you do not specifically configure either the source address or destination address, the default value **0.0.0.0/0** (IPv4 ANY) is used. To use IPv6 ANY (**0::0/128**) as either source or destination address, you must configure it explicitly.

For next-hop-style service sets only, the **ipsec-inside-interface** statement allows you to assign a logical interface to the tunnels established as a result of this match condition. The **inside-service-interface** statement that you can configure at the **[edit services service-set *name* next-hop-service]** hierarchy level allows you to specify .1 and .2 as inside and outside interfaces. However, you can configure multiple adaptive services logical interfaces with the **service-domain inside** statement and use one of them to configure the **ipsec-inside-interface** statement. For more information, see [“Configuring Service Sets to be Applied to Services Interfaces” on page 742](#) and *Interface Properties*.

The Junos OS evaluates the criteria you configure in the **from** statement. If multiple link-type tunnels are configured within the same next-hop-style service set, the **ipsec-inside-interface** value enables the rule lookup module to distinguish a particular tunnel from other tunnels in case the source and destination addresses for all of them are **0.0.0.0/0** (ANY-ANY).



**NOTE:** When you configure the `ipsec-inside-interface` statement, interface-style service sets are not supported.



**NOTE:** Starting with Junos OS Release 14.1, you can configure a maximum of up to 8,000 IPsec tunnels using 6,000 service sets on a router. In such a scenario, you can employ up to 8,000 logical interfaces in your environment and configure IPv4, IPv6, and dead peer detection (DPD) protocols. Until Junos OS Release 13.3, the maximum number of IPsec tunnels supported with 6,000 service sets was 6,000 tunnels.

A special situation is provided by a term containing an “any-any” match condition (usually because the **from** statement is omitted). If there is an any-any match in a tunnel, a flow is not needed, because all flows within this tunnel use the same security association (SA) and packet selectors do not play a significant role. As a result, these tunnels will use packet-based IPsec. This strategy saves some flow resources on the PIC, which can be used for other tunnels that need a flow-based service.

The following configuration example shows an any-any tunnel configuration with no **from** statement in **term-1**. Missing selectors in the **from** clause result in a packet-based IPsec service.

```
services {
  ipsec-vpn {
    rule rule-1 {
      term term-1 {
        then {
          remote-gateway 10.1.0.1;
          dynamic {
            ike-policy ike_policy;
            ipsec-policy ipsec_policy;
          }
        }
      }
    }
    match-direction input;
  }
  .....
}
```

Flowless IPsec service is provided to link-type tunnels with an any-any matching, as well as to dynamic tunnels with any-any matching in both dedicated and shared mode.

For link-type tunnels, a mixture of flowless and flow-based IPsec is supported within a service set. If a service set includes some terms with any-any matching and some terms with selectors in the **from** clause, packet-based service is provided for the any-any tunnels and flow-based service is provided for the other tunnels with selectors.

For non link-type tunnels, if a service set contains both any-any terms and selector-based terms, flow-based service is provided to all the tunnels.

## Configuring Actions in IPsec Rules

To configure actions in an IPsec rule, include the **then** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name]
then {
  anti-replay-window-size bits;
  backup-remote-gateway address;
  clear-dont-fragment-bit;
  copy-dont-fragment-bit;
  set-dont-fragment-bit;
  dynamic {
    ike-policy policy-name;
    ipsec-policy policy-name;
  }
  initiate-dead-peer-detection;
  manual {
    direction (inbound | outbound | bidirectional) {
      authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      auxiliary-spi spi-value;
      encryption {
        algorithm algorithm;
        key (ascii-text key | hexadecimal key);
      }
      protocol (ah | bundle | esp);
      spi spi-value;
    }
  }
  no-anti-replay;
  remote-gateway address;
  syslog;
  tunnel-mtu bytes;
}
```

The principal IPsec actions are to configure a dynamic or manual SA:

- You configure a dynamic SA by including the **dynamic** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level and referencing policies you have configured at the **[edit services ipsec-vpn ipsec]** and **[edit services ipsec-vpn ike]** hierarchy levels; for more information, see [“Configuring Dynamic Security Associations” on page 488](#).
- You configure a manual SA by including the **manual** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level; for more information, see [“Configuring Manual Security Associations” on page 484](#).

You can configure the following additional properties:

- [Enabling IPsec Packet Fragmentation on page 509](#)
- [Configuring Destination Addresses for Dead Peer Detection on page 509](#)

- [Configuring or Disabling IPsec Anti-Replay on page 510](#)
- [Enabling System Log Messages on page 511](#)
- [Specifying the MTU for IPsec Tunnels on page 511](#)

### Enabling IPsec Packet Fragmentation

To enable fragmentation of IP version 4 (IPv4) packets in IPsec tunnels, include the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
  clear-dont-fragment-bit;
```

Setting the **clear-dont-fragment-bit** statement clears the Don't Fragment (DF) bit in the packet header, regardless of the packet size. If the packet size exceeds the tunnel maximum transmission unit (MTU) value, the packet is fragmented before encapsulation. For IPsec tunnels, the default MTU value is 1500 regardless of the interface MTU setting.

In packets that are transmitted through IPsec tunnels, you can enable the value set in the Don't Fragment (DF) bit of the packet entering the tunnel to be copied only to the outer header of the IPsec packet and to not cause any modification to the DF bit in the inner header of the IPsec packet. If the packet size exceeds the tunnel maximum transmission unit (MTU) value, the packet is fragmented before encapsulation. For IPsec tunnels, the default MTU value is 1500 regardless of the interface MTU setting. To copy the DF bit value to only the outer header and not modify the inner header, use the **copy-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level. You can also configure the DF bit to be set only in the outer IPv4 header of the IPsec packet and not be defined in the inner IPv4 header. To configure the DF bit in only the outer header of the IPsec packet and to leave the inner header unmodified, include the **set-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level. These settings apply for static endpoint tunnels and not for dynamic tunnels, for which you need to include the **clear-dont-fragment-bit** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to clear the DF bit in the IPv4 packets that enter the tunnel. These functionalities are supported on MX Series routers with MS-MICs and MS-MPCs.

### Configuring Destination Addresses for Dead Peer Detection

To specify the remote address to which the IPsec traffic is directed, include the **remote-gateway** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
  remote-gateway address;
```

To specify a backup remote address, include the **backup-remote-gateway** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
  backup-remote-gateway address;
```

These two statements support both IPv4 and IPv6 address formats.

Configuring the **backup-remote-gateway** statement enables the dead peer detection (DPD) protocol, which monitors the tunnel state and remote peer availability. When the primary tunnel defined by the **remote-gateway** statement is active, the backup tunnel is in standby mode. If the DPD protocol determines that the primary remote gateway address is no longer reachable, a new tunnel is established to the backup address.

If there is no incoming traffic from a peer during a defined interval of 10 seconds, the router detects a tunnel as inactive. A global timer polls all tunnels every 10 seconds and the Adaptive Services (AS) or Multiservices Physical Interface Card (PIC) sends a message listing any inactive tunnels. If a tunnel becomes inactive, the router takes the following steps to failover to the backup address:

1. The adaptive services message triggers the DPD protocol to send a hello message to the peer.
2. If no acknowledgment is received, two retries are sent at 2-second intervals, and then the tunnel is declared dead.
3. Failover takes place if the tunnel is declared dead or there is an IPsec Phase 1 negotiation timeout. The primary tunnel is put in standby mode and the backup becomes active.
4. If the negotiation to the backup tunnel times out, the router switches back to the primary tunnel. If both peers are down, it tries the failover six times. It then stops failing over and reverts to the original configuration, with the primary tunnel active and the backup in standby mode.

You can also enable triggering of DPD Hello messages without configuring a backup remote gateway by including the **initiate-dead-peer-detection** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
initiate-dead-peer-detection;
```

The monitoring behavior is the same as described for the **backup-remote-gateway** statement. This configuration enables the router to initiate DPD Hellos when a backup IPsec gateway does not exist and clean up the IKE and IPsec SAs in case the IKE peer is not reachable.

If the DPD protocol determines that the primary remote gateway address is no longer reachable, a new tunnel is established to the backup address. However, when you configure **initiate-dead-peer-detection** without a backup remote gateway address and the DPD protocol determines that the primary remote gateway address is no longer reachable, the tunnel is declared dead and IKE and IPsec SAs are cleaned up.

For more information on the DPD protocol, see RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*.

---

### Configuring or Disabling IPsec Anti-Replay

To configure the size of the IPsec antireplay window, include the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
  anti-replay-window-size bits;
```

**anti-replay-window-size** can take values in the range from 64 through 4096 bits. The default value is 64 bits for AS PICs and 128 bits for Multiservices PICs and DPCs. AS PICs can support a maximum replay window size of 1024 bits, whereas Multiservices PICs and DPCs can support a maximum replay window size of 4096 bits. When the software is committing an IPsec configuration, the key management process (kmd) is unable to differentiate between the service interface types. As a result, if the maximum antireplay window size exceeds 1024 for AS PICs, the commit succeeds and no error message is produced. However, the software internally sets the antireplay window size for AS PICs to 1024 bits even if the configured value of the **anti-replay-window-size** is larger.

To disable the IPsec antireplay feature, include the **no-anti-replay** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
  no-anti-replay;
```

By default, antireplay service is enabled. Occasionally this can cause interoperability issues with other vendors' equipment.

### Enabling System Log Messages

To record an alert in the system logging facility, include the **syslog** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
  syslog;
```

### Specifying the MTU for IPsec Tunnels

To configure a specific maximum transmission unit (MTU) value for IPsec tunnels, include the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
  tunnel-mtu bytes;
```



**NOTE:** The **tunnel-mtu** setting is the only place you need to configure an MTU value for IPsec tunnels. Inclusion of an **mtu** setting at the **[edit interfaces *sp-fpc/pic/port* unit *logical-unit-number* family inet]** hierarchy level is not supported.

## Configuring IPsec Rule Sets

The **rule-set** statement defines a collection of IPsec rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the **rule-set** statement at the **[edit services ipsec-vpn]** hierarchy level with a **rule** statement for each rule:

```
[edit services ipsec-vpn]
rule-set rule-set-name {
  rule rule-name;
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing continues to the next rule in the rule set. If none of the rules matches the packet, the packet is dropped by default.

---

## Configuring Dynamic Endpoints for IPsec Tunnels

IPsec tunnels can also be established using *dynamic peer* security gateways, in which the remote ends of tunnels do not have a statically assigned IP address. Since the remote address is not known and might be pulled from an address pool each time the remote host reboots, establishment of the tunnel relies on using IKE **main** mode with either preshared global keys or digital certificates that accept any remote identification value. For more information on IKE policy modes, see [“Configuring the Mode for an IKE Policy” on page 495](#). Both policy-based and link-type tunnels are supported:

- Policy-based tunnels used shared mode.
- Link-type or routed tunnels use dedicated mode. Each tunnel allocates a service interface from a pool of interfaces configured for the dynamic peers. Routing protocols can be configured to run on these service interfaces to learn routes over the IPsec tunnel that is used as a link in this scenario.

This section includes the following topics:

- [Authentication Process on page 512](#)
- [Implicit Dynamic Rules on page 513](#)
- [Reverse Route Insertion on page 513](#)
- [Configuring an IKE Access Profile on page 514](#)
- [Referencing the IKE Access Profile in a Service Set on page 515](#)
- [Configuring the Interface Identifier on page 516](#)
- [Default IKE and IPsec Proposals on page 516](#)

### Authentication Process

The remote (dynamic peer) initiates the negotiations with the local (Juniper Networks) router. The local router uses the default IKE and IPsec policies to match the proposals sent by the remote peer to negotiate the security association (SA) values. Implicit proposals contain a list of all the supported transforms that the local router expects from all the dynamic peers.

If preshared key authentication is used, the preshared key is global for a service set. When seeking the preshared key for the peer, the local router matches the peer's source address against any explicitly configured preshared keys in that service set. If a match is not found,

the local router uses the global preshared key for authentication. This key is the one configured in the IKE access profile referenced by the service set.

Phase 2 of the authentication matches the *proxy identities* of the protected hosts and networks sent by the peer against a list of configured proxy identities. The accepted proxy identity is used to create the dynamic rules for encrypting the traffic. You can configure proxy identities by including the **allowed-proxy-pair** statement in the IKE access profile. If no entry matches, the negotiation is rejected.

If you do not configure the **allowed-proxy-pair** statement, the default value **ANY(0.0.0.0/0)-ANY** is applied, and the local router accepts any proxy identities sent by the peer. Both IPv4 and IPv6 addresses are accepted, but you must configure all IPv6 addresses manually.

Once the phase 2 negotiation completes successfully, the router builds the dynamic rules and inserts the reverse route into the routing table using the accepted proxy identity.

## Implicit Dynamic Rules

After successful negotiation with the dynamic peer, the key management process (kmd) creates a dynamic rule for the accepted phase 2 proxy and applies it on the local AS or Multiservices PIC. The source and destination addresses are specified by the accepted proxy. This rule is used to encrypt traffic directed to one of the end hosts in the phase 2 proxy identity.

The dynamic rule includes an **ipsec-inside-interface** value, which is the interface name assigned to the dynamic tunnel. The **source-address** and **destination-address** values are accepted from the proxy ID. The **match-direction** value is **input** for next-hop-style service sets.



**NOTE:** You do not configure this rule; it is created by the key management process (kmd).

Rule lookup for static tunnels is unaffected by the presence of a dynamic rule; it is performed in the order configured. When a packet is received for a service set, static rules are always matched first.

Dynamic rules are matched after the rule match for static rules has failed.

Response to dead peer detection (DPD) hello messages takes place the same way with dynamic peers as with static peers. Initiating DPD hello messages from dynamic peers is not supported. For more information on DPD, see [“Configuring Destination Addresses for Dead Peer Detection” on page 509](#).

## Reverse Route Insertion

Static routes are automatically inserted into the route table for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created based on the remote proxy network and mask sent by the peer and is inserted in the relevant route table after successful phase 1 and phase 2 negotiations.

The route preference for each static reverse route is 1. This value is necessary to avoid conflict with similar routes that might be added by the routing protocol process (rpd).

No routes are added if the accepted remote proxy address is the default (**0.0.0.0/0**). In this case you can run routing protocols over the IPsec tunnel to learn routes and add static routes for the traffic you want to be protected over this tunnel.

For next-hop-style service sets, the reverse routes include next hops pointing to the locations specified by the **inside-service-interface** statement.

The route table in which to insert these routes depends on where the **inside-service-interface** location is listed. If these interfaces are present in a VPN routing and forwarding (VRF) instance, then routes are added to the corresponding VRF table; otherwise, the routes are added to **inet.0**.



**NOTE:** Reverse route insertion takes place only for tunnels to dynamic peers. These routes are added only for next-hop-style service sets.

## Configuring an IKE Access Profile

You can configure only one tunnel profile per service set for all dynamic peers. The configured preshared key in the profile is used for IKE authentication of all dynamic peers terminating in that service set. Alternatively, you can include the **ike-policy** statement to reference an IKE policy you define with either specific identification values or a wildcard (the **any-remote-id** option). You configure the IKE policy at the **[edit services ipsec-vpn ike]** hierarchy level; for more information, see “[Configuring IKE Policies](#)” on page 493.

The IKE tunnel profile specifies all the information needed to complete the IKE negotiation. Each protocol has its own statement hierarchy within the client statement to configure protocol-specific attribute value pairs, but only one client configuration is allowed for each profile. The following is the configuration at the **[edit access]** hierarchy level; for more information on access profiles, see the *Junos OS Administration Library for Routing Devices*.

```
[edit access]
profile profile-name {
  client * {
    ike {
      allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
      }
      pre-shared-key (ascii-text key-string | hexadecimal key-string);
      ike-policy policy-name;
      interface-id <string-value>;
      ipsec-policy ipsec-policy;
    }
  }
}
```



**NOTE:** For dynamic peers, the Junos OS supports the IKE main mode with either the preshared key method of authentication or an IKE access profile that uses a local digital certificate.

- In preshared key mode, the IP address is used to identify a tunnel peer to get the preshared key information. The client value \* (wildcard) means that configuration within this profile is valid for all dynamic peers terminating within the service set accessing this profile.
- In digital certificate mode, the IKE policy defines which remote identification values are allowed; for more information, see [“Configuring IKE Policies” on page 493](#).

The following statements make up the IKE profile:

- **allowed-proxy-pair**—During phase 2 IKE negotiation, the remote peer supplies its network address (**remote**) and its peer’s network address (**local**). Since multiple dynamic tunnels are authenticated through the same mechanism, this statement must include the list of possible combinations. If the dynamic peer does not present a valid combination, the phase 2 IKE negotiation fails.

By default, **remote 0.0.0.0/0 local 0.0.0.0/0** is used if no values are configured. Both IPv4 and IPv6 address formats are supported in this configuration, but there are no default IPv6 addresses. You must specify even **0::0/0**.

- **pre-shared-key**—Key used to authenticate the dynamic peer during IKE phase 1 negotiation. This key is known to both ends through an out-of-band secure mechanism. You can configure the value either in **hexadecimal** or **ascii-text** format. It is a mandatory value.
- **ike-policy**—Policy that defines the remote identification values corresponding to the allowed dynamic peers; can contain a wildcard value **any-remote-id** for use in dynamic endpoint configurations only.
- **interface-id**—Interface identifier, a mandatory attribute used to derive the logical service interface information for the session.
- **ipsec-policy**—Name of the IPsec policy that defines the IPsec policy information for the session. You define the IPsec policy at the **[edit services ipsec-vpn ipsec policy policy-name]** hierarchy level. If no policy is set, any policy proposed by the dynamic peer is accepted.

## Referencing the IKE Access Profile in a Service Set

To complete the configuration, you need to reference the IKE access profile configured at the **[edit access]** hierarchy level. To do this, include the **ike-access-profile** statement at the **[edit services service-set name ipsec-vpn-options]** hierarchy level:

```
[edit services service-set name]
ipsec-vpn-options {
    local-gateway address;
    ike-access-profile profile-name;
```

```

}
next-hop-service {
  inside-service-interface interface-name;
  outside-service-interface interface-name;
}

```

The **ike-access-profile** statement must reference the same name as the **profile** statement you configured for IKE access at the **[edit access]** hierarchy level. You can reference only one access profile in each service set. This profile is used to negotiate IKE and IPsec security associations with dynamic peers only.



**NOTE:** If you configure an IKE access profile in a service set, no other service set can share the same **local-gateway** address.

Also, you must configure a separate service set for each VRF instance. All interfaces referenced by the **ipsec-inside-interface** statement within a service set must belong to the same VRF instance.

## Configuring the Interface Identifier

You can configure an interface identifier for a group of dynamic peers, which specifies which adaptive services logical interface(s) take part in the dynamic IPsec negotiation. By assigning the same interface identifier to multiple logical interfaces, you can create a pool of interfaces for this purpose. To configure an interface identifier, include the **ipsec-interface-id** statement and the **dedicated** or **shared** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* dial-options]** hierarchy level:

```

[edit interfaces interface-name unit logical-unit-number dial-options]
ipsec-interface-id identifier;
(dedicated | shared);

```

Specifying the interface identifier in the **dial-options** statement makes this logical interface part of the pool identified by the **ipsec-interface-id** statement.



**NOTE:** Only one interface identifier can be specified at a time. You can include the **ipsec-interface-id** statement or the **l2tp-interface-id** statement, but not both.

If you configure **shared** mode, it enables one logical interface to be shared across multiple tunnels. The **dedicated** statement specifies that the logical interface is used in a dedicated mode, which is necessary when you are configuring an IPsec link-type tunnel. You must include the **dedicated** statement when you specify an **ipsec-interface-id** value.

## Default IKE and IPsec Proposals

The software includes implicit default IKE and IPsec proposals to match the proposals sent by the dynamic peers. The values are shown in [Table 29 on page 517](#); if more than one value is shown, the first value is the default. For more information on IKE proposals,

see “Configuring IKE Proposals” on page 489; for more information on IPsec proposals, see “Configuring IPsec Proposals” on page 499.



**NOTE:** RSA certificates are not supported with dynamic endpoint configuration.

**Table 29: Default IKE and IPsec Proposals for Dynamic Negotiations**

Statement Name	Values
<b>Implicit IKE Proposal</b>	
authentication-method	pre-shared keys
dh-group	group1, group2, group5, group14
authentication-algorithm	sha1, md5, sha-256
encryption-algorithm	3des-cbc, des-cbc, aes-128, aes-192, aes-256
lifetime-seconds	3600 seconds
<b>Implicit IPsec Proposal</b>	
protocol	esp, ah, bundle
authentication-algorithm	hmac-sha1-96, hmac-md5-96
encryption-algorithm	3des-cbc, des-cbc, aes-128, aes-192, aes-256
lifetime-seconds	28,800 seconds (8 hours)

## Tracing IPsec Operations

Trace operations track IPsec events and record them in a log file in the `/var/log` directory. By default, this file is named `/var/log/kmd`.

To trace IPsec operations, include the `traceoptions` statement at the `[edit services ipsec-vpn]` hierarchy level:

```
[edit services ipsec-vpn]
traceoptions {
  file <filename> <files number> <match regular-expression> <size bytes> <world-readable |
    no-world-readable>;
  flag <flag>;
  level <level>;
  no-remote-trace;
}
```

You can specify the following IPsec tracing flags:

- **all**—Trace everything.
- **certificates**—Trace certificates events.
- **database**—Trace security associations database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **snmp**—Trace SNMP operations.
- **timer**—Trace internal timer events.

The **level** statement sets the key management process (kmd) tracing level. The following values are supported:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

## Disabling IPsec Tunnel Endpoint in Traceroute

If you include the **no-ipsec-tunnel-in-traceroute** statement at the **[edit services ipsec-vpn]** hierarchy level, the IPsec tunnel is not treated as a next hop and TTL is not decremented. Also, if the TTL reaches zero, an ICMP time exceeded message is not generated.

```
[edit services ipsec-vpn]
no-ipsec-tunnel-in-traceroute;
```



**NOTE:** This functionality is also provided by the **passive-mode-tunneling** statement described in “[Configuring IPsec Service Sets](#)” on page 748. You can use the **no-ipsec-tunnel-in-traceroute** statement in specific scenarios in which the IPsec tunnel should not be treated as a next hop and passive mode is not desired.

## Tracing IPsec PKI Operations

Trace operations track IPsec PKI events and record them in a log file in the **/var/log** directory. By default, this file is named **/var/log/pkid**.

To trace IPsec PKI operations, include the **traceoptions** statement at the **[edit security pki]** hierarchy level:

```
[edit security pki]
traceoptions {
  file filename <files number> <match regular-expression> <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag (all | certificate-verification | enrollment | online-crl-check);
}
```

You can specify the following PKI tracing flags:

- **all**—Trace everything.
- **certificates**—Trace certificates events.
- **database**—Trace security associations database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **snmp**—Trace SNMP operations.
- **timer**—Trace internal timer events.

## Configuring IPsec Using the Extension-Provider Package

Starting with Junos OS Release 11.4, IPsec is supported by the extension-provider packages. IPsec on the extension-provider package is supported on all M Series, T Series, and MX Series routers with Multiservices 100, Multiservices 400 PICs, and Multiservices DPCs.



**NOTE:** In Junos OS releases earlier than 12.3, the extension-provider packages were variously referred to as Junos Services Framework (JSF), MP-SDK, and eJunos.

IPsec on the extension-provider package has the following limitations:

- IPsec on the extension-provider package supports only policies negotiated between dynamic peer security gateways in which the remote ends of tunnels do not have a statically assigned IP address (Dynamic Endpoints).
- Encapsulating Security Payload (ESP) is the only protocol that is supported for protecting IP traffic.
- IPsec on the extension-provider package does not support IPv6.

To enable IPSec for the extension-provider package on the adaptive services interface, configure the **object-cache-size**, **policy-db-size**, and **package** statements at the **[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]** hierarchy level. For the IPSec plugin in the extension-provider package, **package-name** in the **package package-name** statement is **jservices-ipsec**.

For more information about the Services SDK, see the *SDK Applications Configuration Guide and Command Reference*.

The following example shows how to enable IPSec for the extension-provider package on the adaptive services interface:

```
chassis fpc 1 {
  pic 2 {
    adaptive-services {
      service-package {
        extension-provider {
          control-cores 1;
          data-cores 7;
          object-cache-size 1280;
          policy-db-size 64;
          package jservices-crypto-base;
          package jservices-ipsec;
        }
      }
    }
  }
}
```

Configure the inside and outside interfaces for next-hop-style service sets:

```
service-set abc {
  next-hop-service {
    inside-service-interface ms-0/2/0.1; # Name and logical unit number of the service
    interface associated with the service set applied inside the network.
    outside-service-interface ms-0/2/0.2; # Name and logical unit number of the service
    interface associated with the service set applied outside the network.
  }
}
```

**Related Documentation**

- [Junos VPN Site Secure](#)

---

## Examples: Configuring IPsec Services

See the following sections:

- [Example: Configuring Statically Assigned Tunnels on page 521](#)
- [Example: Configuring Dynamically Assigned Tunnels on page 524](#)
- [Multitask Example: Configuring IPsec Services on page 528](#)

## Example: Configuring Statically Assigned Tunnels

Following is the configuration of the provider edge (PE) router, demonstrating the usage of next-hop service sets and dynamic SA configuration:

```
[edit interfaces]
so-0/0/0 {
  no-keepalives;
  encapsulation cisco-hdlc;
  unit 0 {
    family inet {
      address 10.6.6.6/32;
    }
  }
}
so-2/2/0 {
  description "teller so-0/2/0";
  no-keepalives;
  encapsulation cisco-hdlc;
  unit 0 {
    family inet {
      address 10.21.1.1/16;
    }
  }
}
sp-3/1/0 {
  unit 0 {
    family inet {
      address 10.7.7.7/32;
    }
  }
  unit 1 {
    family inet;
    service-domain inside;
  }
  unit 2 {
    family inet;
    service-domain outside;
  }
}
[edit policy-options]
policy-statement vpn-export {
  then {
    community add vpn-comm;
    accept;
  }
}
policy-statement vpn-import {
  term a {
    from community vpn-comm;
    then accept;
  }
}
community vpn-comm members target:100:20;
[edit routing-instances]
```

```
vrf {
  instance-type vrf;
  interface sp-3/1/0.1; # Inside sp interface
  interface so-0/0/0.0;
  route-distinguisher 192.168.0.1:1;
  vrf-import vpn-import;
  vrf-export vpn-export;
  routing-options {
    static {
      route 10.0.0.0/0 next-hop so-0/0/0.0;
      route 10.11.11.1/32 next-hop so-0/0/0.0;
      route 10.8.8.1/32 next-hop sp-3/1/0.1;
    }
  }
}
[edit services]
ipsec-vpn {
  rule rule-1 {
    term term-1 {
      then {
        remote-gateway 10.21.2.1;
        dynamic {
          ike-policy ike-policy;
        }
      }
    }
  }
  match-direction input;
}
ike {
  policy ike-policy {
    pre-shared-key ascii-text "$9$ExmcSeMWxdVYBI";
  }
}
}
service-set service-set-1 {
  ipsec-vpn {
    local-gateway 10.21.1.1;
  }
  ipsec-vpn-rules rule-1;
  next-hop-service {
    inside-service-interface sp-3/1/0.1;
    outside-service-interface sp-3/1/0.2;
  }
}
```

Following is an example for configuring multiple link-type tunnels to static peers using a single next-hop style service set:

```
services ipsec-vpn {
  rule demo-rule {
    term term-0 {
      from {
        ipsec-inside-interface sp-0/0/0.1;
      }
      then {
        remote-gateway 10.2.2.2;
      }
    }
  }
}
```

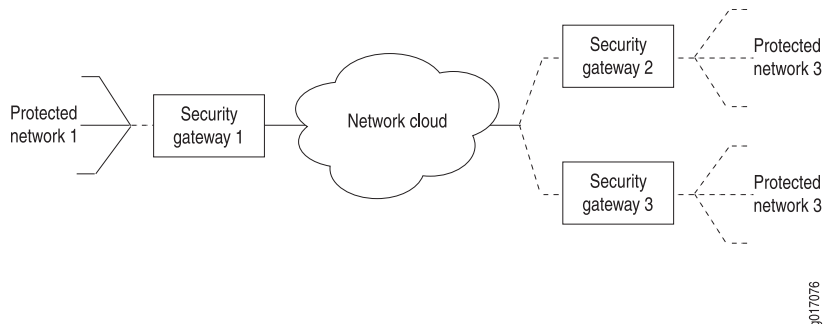
```
        dynamic {
            ike-policy demo-ike-policy;
        }
    }
}
term term-1 {
    from {
        ipsec-inside-interface sp-0/0/0.3;
    }
    then {
        remote-gateway 10.3.3.3;
        dynamic {
            ike-policy demo-ike-policy;
        }
    }
}
}
match-direction input;
}
services {
    service-set demo-service-set {
        next-hop-service {
            inside-service-interface sp-0/0/0.1;
            outside-service-interface sp-0/0/0.2;
        }
        ipsec-vpn-options {
            local-gateway 10.1.1.1;
        }
        ipsec-rules demo-rule;
    }
}
interfaces sp-0/0/0 {
    unit 0 {
        family inet;
    }
    unit 1 {
        family inet;
        service-domain inside;
    }
    unit 2 {
        family inet;
        service-domain outside;
    }
    unit 3 {
        family inet;
        service-domain inside;
    }
    unit 4 {
        family inet;
        service-domain inside;
    }
}
```

## Example: Configuring Dynamically Assigned Tunnels

The following examples are based on this network configuration (see [Figure 17 on page 524](#)):

- A local network N-1 behind security gateway SG-1, a Juniper Networks router terminating static as well as dynamic peer endpoints. The tunnel termination address on SG-1 is 10.1.1.1 and the local network address is 172.16.1.0/24.
- Two remote peer routers that obtain addresses from an ISP pool and run RFC-compliant IKE. Remote network N-2 has address 172.16.2.0/24 and resides behind security gateway SG-2 with tunnel termination address 10.2.2.2. Remote network N-3 has address 172.16.3.0/24 and resides behind security gateway SG-3 with tunnel termination address 10.3.3.3.

**Figure 17: IPsec Dynamic Endpoint Tunneling Topology**



The examples in this section show the following configurations:

- [Configuring a Next-Hop Style Service Set with Link-Type Tunnels on page 524](#)
- [Configuring a Next-Hop Style Service-Set with Policy-Based Tunnels on page 526](#)



**NOTE:** All the configurations are given for the Juniper Networks router terminating dynamic endpoint connections.

### Configuring a Next-Hop Style Service Set with Link-Type Tunnels

```
access {
  profile demo-access-profile client * {
    ike {
      allowed-proxy-pair {
        remote 0.0.0.0/0 local 0.0.0.0/0; # ANY to ANY
      }
      pre-shared-key {
        ascii-text keyfordynamicpeers;
      }
      interface-id demo-ipsec-interface-id;
    }
  }
}
services {
  service-set demo-service-set {
    next-hop-service {
```

```

        inside-service-interface sp-1/0/0.1;
        outside-service-interface sp-1/0/0.2;
    }
    ipsec-vpn-options {
        local-gateway 10.1.1.1;
        ike-access-profile demo-ike-access-profile;
    }
}
}
}

```



**NOTE:** Including the `ike-access-profile` statement enables the software to incorporate implicit proposals for dynamic endpoint authentication. You do not need to configure IKE or IPsec proposals explicitly.

```

interfaces {
    sp-0/0/0 {
        unit 0 {
            family inet;
        }
        unit 1 {
            family inet;
            service-domain inside;
        }
        unit 2 {
            family inet;
            service-domain outside;
        }
        unit 3 {
            family inet;
            service-domain inside;
            dial-options {
                ipsec-interface-id demo-ipsec-interface-id;
                dedicated;
            }
        }
        unit 4 {
            family inet;
            service-domain inside;
            dial-options {
                ipsec-interface-id demo-ipsec-interface-id;
                dedicated;
            }
        }
    }
}
}

```

The following results are obtained:

- Reverse routes inserted after successful negotiation:  
None
- Routes learned by routing protocol:

172.16.2.0/24

172.16.3.0/24

- Dynamic implicit rules created after successful negotiation:

```
rule: junos-dynamic-rule-0
term: term-0
  local-gateway-address : 10.1.1.1 #Tunnel termination address on SG-1
  remote-gateway-address: 10.2.2.2 #Tunnel termination address on SG-2
  source-address : 0.0.0.0/0
  destination-address : 0.0.0.0/0
ipsec-inside-interface: sp-0/0/0.3
term: term-1
  local-gateway-address : 10.1.1.1 #Tunnel termination address on SG-1
  remote-gateway-address: 10.3.3.3 #Tunnel termination address on SG-3
  source-address : 0.0.0.0/0
  destination-address : 0.0.0.0/0
ipsec-inside-interface: sp-0/0/0.4
match-direction: input
```

#### Configuring a Next-Hop Style Service-Set with Policy-Based Tunnels

```
access {
  profile demo-access-profile client * {
    ike {
      allowed-proxy-pair {
        remote 172.16.2.0/24 local 172.16.1.0/24; #N-2 <==> #N-1
        remote 172.16.3.0/24 local 172.16.1.0/24; #N-3 <==> #N-1
      }
      pre-shared-key {
        ascii-text keyfordynamicpeers;
      }
      interface-id demo-ipsec-interface-id;
    }
  }
}
services {
  service-set demo-service-set {
    next-hop-service {
      inside-service-interface sp-1/0/0.1;
      outside-service-interface sp-1/0/0.2;
    }
    ipsec-vpn-options {
      local-gateway 10.1.1.1;
    }
    ike-access-profile demo-ike-access-profile;
  }
}
```



**NOTE:** Including the `ike-access-profile` statement enables the software to incorporate implicit proposals for dynamic endpoint authentication. You do not need to configure IKE or IPsec proposals explicitly.

```
interfaces {
  sp-0/0/0 {
```

```

unit 0 {
    family inet;
}
unit 1 {
    family inet;
    service-domain inside;
}
unit 2 {
    family inet;
    service-domain outside;
}
unit 3 {
    family inet;
    service-domain inside;
    dial-options {
        ipsec-interface-id demo-ipsec-interface-id;
        mode shared;
    }
}
}
}
# VRF configuration, if not inet.0
routing-instances {
    demo-vrf {
        instance-type vrf;
        interface sp-0/0/0.1;
        interface sp-0/0/0.3;
        .....
    }
}

```

The following results are obtained:

- Reverse routes injected after successful negotiation:

```

demo-vrf.inet.0: .... # Routing instance
172.11.0.0/24 *[Static/1]..
> via sp-0/0/0.3
172.12.0.0/24 *[Static/1]..
> via sp-0/0/0.3

```

- Dynamic implicit rules created after successful negotiation:

```

rule: junos-dynamic-rule-0
term: term-0
  local-gateway-address : 10.1.1.1 #Tunnel termination address on SG-1
  remote-gateway-address: 10.2.2.2 #Tunnel termination address on SG-2
  source-address : 172.16.1.0/24
  destination-address : 172.16.2.0/24
  ipsec-inside-interface: sp-0/0/0.3
term: term-1
  local-gateway-address : 10.1.1.1 #Tunnel termination address on SG-1
  remote-gateway-address: 10.3.3.3 #Tunnel termination address on SG-3
  source-address : 172.16.1.0/24
  destination-address : 172.16.3.0/24
  ipsec-inside-interface: sp-0/0/0.3
match-direction: input

```

## Multitask Example: Configuring IPsec Services

The following example-based instructions show how to configure IPsec services. The configuration involves defining an IKE policy, an IPsec policy, IPsec rules, trace options, and service sets.

This topic includes the following tasks:

1. [Configuring the IKE Proposal on page 528](#)
2. [Configuring the IKE Policy \(and Referencing the IKE Proposal\) on page 529](#)
3. [Configuring the IPsec Proposal on page 529](#)
4. [Configuring the IPsec Policy \(and Referencing the IPsec Proposal\) on page 530](#)
5. [Configuring the IPsec Rule \(and Referencing the IKE and IPsec Policies\) on page 531](#)
6. [Configuring IPsec Trace Options on page 532](#)
7. [Configuring the Access Profile \(and Referencing the IKE and IPsec Policies\) on page 532](#)
8. [Configuring the Service Set \(and Referencing the IKE Profile and the IPsec Rule\) on page 533](#)

---

### Configuring the IKE Proposal

The IKE proposal configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway. For more information about IKE proposals, see [“Configuring IKE Proposals” on page 489](#).

To define the IKE proposal:

1. In configuration mode, go to the following hierarchy level:  

```
user@host# edit services ipsec-vpn
```
2. Configure the authentication method, which is **pre-shared keys** in this example:  

```
[edit services ipsec-vpn]  
user@host# set ike proposal test-IKE-proposal authentication-method pre-shared-keys
```
3. Configure the Diffie-Hellman Group and specify a name—for example, **group1**:  

```
[edit services ipsec-vpn]  
user@host# set ike proposal test-IKE-proposal dh-group group1
```
4. Configure the authentication algorithm, which is **sha1** in this example:  

```
[edit services ipsec-vpn]  
user@host# set ike proposal test-IKE-proposal authentication-algorithm sha1
```
5. Configure the encryption algorithm, which is **aes-256-cbc** in this example:  

```
[edit services ipsec-vpn]  
user@host# set ike proposal test-IKE-proposal encryption-algorithm aes-256-cbc
```

The following sample output shows the configuration of the IKE proposal:

```
[edit services ipsec-vpn]  
user@host# show ike  
proposal test-IKE-proposal {
```

```

authentication-method pre-shared-keys;
dh-group group1;
authentication-algorithm sha1;
encryption-algorithm aes-256-cbc;
}

```

### Configuring the IKE Policy (and Referencing the IKE Proposal)

The IKE policy configuration defines the proposal, mode, addresses, and other security parameters used during IKE negotiation. For more information about IKE policies, see [“Configuring IKE Policies” on page 493](#).

To define the IKE policy and reference the IKE proposal:

1. In configuration mode, go to the following hierarchy level:  

```
user@host# edit services ipsec-vpn
```
2. Configure the IKE first phase mode—for example, **main**:  

```
[edit services ipsec-vpn]
user@host# set ike policy test-IKE-policy mode main
```
3. Configure the proposal, which is **test-IKE-proposal** in this example:  

```
[edit services ipsec-vpn]
user@host# set ike policy test-IKE-policy proposals test-IKE-proposal
```
4. Configure the local identification with an IPv4 address—for example, **192.168.255.2**:  

```
[edit services ipsec-vpn]
user@host# set ike policy test-IKE-policy local-id ipv4_addr 192.168.255.2
```
5. Configure the preshared key in ASCII text format, which is **TEST** in this example:  

```
[edit services ipsec-vpn]
user@host# set ike policy test-IKE-policy pre-shared-key ascii-text TEST
```

The following sample output shows the configuration of the IKE policy:

```

[edit services ipsec-vpn]
user@host# show ike
policy test-IKE-policy {
    mode main;
    proposals test-IKE-proposal;
    local-id ipv4_addr 192.168.255.2;
    pre-shared-key ascii-text TEST;
}

```

### Configuring the IPsec Proposal

The IPsec proposal configuration defines the protocols and algorithms (security services) that are required to negotiate with the remote IPsec peer. For more information about IPsec proposals, see [“Configuring IPsec Proposals” on page 499](#).

To define the IPsec proposal:

1. In configuration mode, go to the following hierarchy level:  

```
user@host# edit services ipsec-vpn
```

2. Configure the IPsec protocol for the proposal—for example, **esp**:

```
[edit services ipsec-vpn]
user@host# set ipsec proposal test-IPsec-proposal protocol esp
```

3. Configure the authentication algorithm for the proposal, which is **hmac-sha1-96** in this example:

```
[edit services ipsec-vpn]
user@host# set ipsec proposal test-IPsec-proposal authentication-algorithm
hmac-sha1-96
```

4. Configure the encryption algorithm for the proposal, which is **aes-256-cbc** in this example:

```
[edit services ipsec-vpn]
user@host# set ipsec proposal test-IPsec-proposal encryption-algorithm aes-256-cbc
```

The following sample output shows the configuration of the IPsec proposal:

```
[edit services ipsec-vpn]
user@host# show ike
proposal test-IPsec-proposal {
  protocol esp;
  authentication-algorithm hmac-sha1-96;
  encryption-algorithm aes-256-cbc;
}
```

---

### Configuring the IPsec Policy (and Referencing the IPsec Proposal)

---

The IPsec policy configuration defines a combination of security parameters (IPsec proposals) used during IPsec negotiation. It defines PFS and the proposals needed for the connection. For more information about IPsec policies, see [“Configuring IPsec Policies” on page 501](#).

To define the IPsec policy and reference the IPsec proposal:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit services ipsec-vpn
```

2. Configure the keys for perfect forward secrecy in the IPsec policy—for example, **group1**:

```
[edit services ipsec-vpn]
user@host# set ipsec policy test-IPsec-policy perfect-forward-secretcy keys group1
```

3. Configure a set of IPsec proposals in the IPsec policy—for example, **test-IPsec-proposal**:

```
[edit services ipsec-vpn]
user@host# set ipsec policy test-IPsec-policy proposals test-IPsec-proposal
```

The following sample output shows the configuration of the IPsec policy:

```
[edit services ipsec-vpn]
user@host# show ipsec policy test-IPsec-policy
perfect-forward-secretcy {
  keys group1;
}
proposals test-IPsec-proposal;
```

### Configuring the IPsec Rule (and Referencing the IKE and IPsec Policies)

The IPsec rule configuration defines the direction that specifies whether the match is applied on the input or output side of the interface. The configuration also consists of a set of terms that specify the match conditions and applications that are included and excluded and also specify the actions and action modifiers to be performed by the router software. For more information about IPsec rules, see [“Configuring IPsec Rules” on page 504](#).

To define the IPsec rule and reference the IKE and IPsec policies:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit services ipsec-vpn
```

2. Configure the IP destination address for the IPsec term in the IPsec rule—for example, **192.168.255.2/32**:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule term 10 from destination-address 192.168.255.2/32
```

3. Configure the remote gateway address for the IPsec term in the IPsec rule—for example, **0.0.0.0**:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule term 10 then remote-gateway 0.0.0.0
```

4. Configure a dynamic security association for IKE policy for the IPsec term in the IPsec rule, which is **test-IKE-policy** in this example:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule term 10 then dynamic ike-policy test-IKE-policy
```

5. Configure a dynamic security association for IKE proposal for the IPsec term in the IPsec rule, which is **test-IPsec-proposal** in this example:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule term 10 then dynamic ipsec-policy test-IPsec-policy
```

6. Configure a direction for which the rule match is being applied in the IPsec rule—for example, **input**:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule match-direction input
```

The following sample output shows the configuration of the IPsec rule:

```
[edit services ipsec-vpn]
user@host# show rule test-IPsec-rule
term 10 {
  from {
    destination-address {
      192.168.255.2/32;
    }
  }
  then {
    remote-gateway 0.0.0.0;
    dynamic {
      ike-policy test-IKE-policy;
    }
  }
}
```

```
        ipsec-policy test-IPsec-policy;
    }
}
match-direction input;
```

### Configuring IPsec Trace Options

---

The IPsec trace options configuration tracks IPsec events and records them in a log file in the **/var/log** directory. By default, this file is named **/var/log/kmd**. For more information about IPsec rules, see [“Tracing IPsec Operations” on page 517](#).

To define the IPsec trace options:

1. In configuration mode, go to the following hierarchy level:  

```
user@host# edit services ipsec-vpn
```
2. Configure the trace file, which is **ipsec.log** in this example:  

```
[edit services ipsec-vpn]
user@host# set traceoptions file ipsec.log
```
3. Configure all the tracing parameters with the option **all** in this example:  

```
[edit services ipsec-vpn]
user@host# set traceoptions flag all
```

The following sample output shows the configuration of the IPsec trace options:

```
[edit services ipsec-vpn]
user@host# show traceoptions
file ipsec.log;
flag all;
```

### Configuring the Access Profile (and Referencing the IKE and IPsec Policies)

---

The access profile configuration defines the access profile and references the IKE and IPsec policies. For more information about access profile, see *Configuring an IKE Access Profile*.

To define the access profile and reference the IKE and IPsec policies:

1. In configuration mode, go to the following hierarchy level:  

```
user@host# [edit access]
```
2. Configure the list of local and remote proxy identity pairs with the **allowed-proxy-pair** option. In this example, **10.0.0.0/24** is the IP address for local proxy identity and **10.0.1.0/24** is the IP address for remote proxy identity:  

```
[edit access]
user@host# set profile IKE-profile-TEST client * ike allowed-proxy-pair local
10.0.0.0/24 remote 10.0.1.0/24
```
3. Configure the IKE policy—for example, **test-IKE-policy**:  

```
[edit access]
user@host# set profile IKE-profile-TEST client * ike ike-policy test-IKE-policy
```

4. Configure the IPsec policy—for example, **test-IPsec-policy**:

```
[edit access]
user@host# set profile IKE-profile-TEST client * ike ipsec-policy test-IPsec-policy
```

5. Configure the identity of logical service interface pool, which is **TEST-intf** in this example:

```
[edit access]
user@host# set profile IKE-profile-TEST client * ike interface-id TEST-intf
```

The following sample output shows the configuration of the access profile:

```
[edit access]
user@host# show
profile IKE-profile-TEST {
  client * {
    ike {
      allowed-proxy-pair local 10.0.0.0/24 remote 10.0.1.0/24;
      ike-policy test-IKE-policy;
      ipsec-policy test-IPsec-policy; # new statement
      interface-id TEST-intf;
    }
  }
}
```

### Configuring the Service Set (and Referencing the IKE Profile and the IPsec Rule)

The service set configuration defines IPsec service sets that require additional specifications and references the IKE profile and the IPsec rule. For more information about IPsec service sets, see [“Configuring IPsec Service Sets” on page 748](#).

To define the service set configuration with the next-hop service sets and IPsec VPN options:

1. In configuration mode, go to the following hierarchy level:

```
user@host# [edit services]
```

2. Configure a service set with parameters for next hop service interfaces for the inside network—for example, **sp-1/2/0.1**:

```
[edit services]
user@host# set service-set TEST next-hop-service inside-service-interface sp-1/2/0.1
```

3. Configure a service set with parameters for next hop service interfaces for the outside network—for example, **sp-1/2/0.2**:

```
[edit services]
user@host# set service-set TEST next-hop-service outside-service-interface sp-1/2/0.2
```

4. Configure the IPsec VPN options with the address and routing instance for the local gateway—for example, **192.168.255.2**:

```
[edit services]
user@host# set service-set TEST ipsec-vpn-options local-gateway 192.168.255.2
```

5. Configure the IPsec VPN options with the IKE access profile for dynamic peers, which is **IKE-profile-TEST** in this example:

```
[edit services]
```

```
user@host# set service-set TEST ipsec-vpn-options ike-access-profile IKE-profile-TEST
```

6. Configure a service set with IPsec VPN rules, which is **test-IPsec-rule** in this example:

```
[edit services]
```

```
user@host# set service-set TEST ipsec-vpn-rules test-IPsec-rule
```

The following sample output shows the configuration of the service set configuration referencing the IKE profile and the IPsec rule:

```
[edit services]user@host# show service-set TEST
next-hop-service {
    inside-service-interface sp-1/2/0.1;
    outside-service-interface sp-1/2/0.2;
}
ipsec-vpn-options {
    local-gateway 192.168.255.2;
    ike-access-profile IKE-profile-TEST;
}
ipsec-vpn-rules test-IPsec-rule;
```

# Summary of IPsec Services Configuration Statements

The following sections explain each of the IP Security (IPsec) services statements. The statements are organized alphabetically.

- [anti-replay-window-size \(Services IPsec VPN\) on page 537](#)
- [authentication \(Services IPsec VPN\) on page 538](#)
- [authentication-method \(Services IPsec VPN\) on page 540](#)
- [auxiliary-spi \(Services IPsec VPN\) on page 541](#)
- [backup-remote-gateway on page 541](#)
- [clear-dont-fragment-bit \(Services IPsec VPN\) on page 542](#)
- [clear-ike-sas-on-pic-restart on page 542](#)
- [clear-ipsec-sas-on-pic-restart on page 543](#)
- [copy-dont-fragment-bit \(Services IPsec VPN\) on page 543](#)
- [description \(Services IPsec VPN\) on page 544](#)
- [destination-address \(Services IPsec VPN\) on page 544](#)
- [dh-group on page 545](#)
- [direction on page 546](#)
- [dynamic on page 547](#)
- [encryption on page 548](#)
- [encryption-algorithm \(Services IPsec VPN\) on page 549](#)
- [from \(Services IPsec VPN\) on page 550](#)
- [ike on page 551](#)
- [initiate-dead-peer-detection on page 552](#)
- [ipsec \(Services IPsec VPN\) on page 553](#)
- [ipsec-inside-interface on page 553](#)
- [lifetime-seconds \(Services IPsec VPN\) on page 554](#)
- [local-certificate \(Services IPsec VPN\) on page 554](#)
- [local-id on page 555](#)

- [manual](#) on page 556
- [match-direction \(Services IPsec VPN\)](#) on page 556
- [mode \(Services IPsec VPN\)](#) on page 557
- [no-anti-replay \(Services IPsec VPN\)](#) on page 557
- [no-ipsec-tunnel-in-traceroute](#) on page 558
- [perfect-forward-secrecy \(Services IPsec VPN\)](#) on page 558
- [pre-shared-key \(Services IKE\)](#) on page 560
- [proposals](#) on page 562
- [protocol](#) on page 563
- [remote-gateway](#) on page 563
- [remote-id](#) on page 564
- [rule \(Services IPsec VPN\)](#) on page 565
- [rule-set \(Services IPsec VPN\)](#) on page 566
- [services \(IPsec VPN\)](#) on page 566
- [set-dont-fragment-bit \(Services IPsec VPN\)](#) on page 567
- [source-address \(Services IPsec VPN\)](#) on page 567
- [spi](#) on page 568
- [syslog \(Services IPsec VPN\)](#) on page 568
- [term \(Services IPsec VPN\)](#) on page 569
- [then \(Services IPsec VPN\)](#) on page 570
- [traceoptions \(Services IPsec VPN\)](#) on page 571
- [traceoptions \(PKI\)](#) on page 573
- [tunnel-mtu \(Services IPsec VPN\)](#) on page 574
- [version \(IKE\)](#) on page 575


## anti-replay-window-size (Services IPsec VPN)

---

<b>Syntax</b>	anti-replay-window-size <i>bits</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify the size of the IPsec antireplay window.
<b>Options</b>	<b>bits</b> —Size of the antireplay window, in bits. <b>Default:</b> 64 bits (AS PICs), 128 bits (Multiservices PICs and DPCs) <b>Range:</b> 64 through 4096 bits
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Rules</i></li></ul>

## authentication (Services IPsec VPN)

---

<b>Syntax</b>	<pre>authentication {   algorithm (hmac-md5-96   hmac-sha1-96   hmac-sha-256-128);   key (ascii-text key   hexadecimal key); }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> <a href="#">manual</a> <a href="#">direction</a> <i>direction</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure IPsec authentication parameters for a manual security association (SA).
<b>Options</b>	<p><b>algorithm</b>—Hash algorithm that authenticates packet data. The algorithm can be one of the following:</p> <ul style="list-style-type: none"><li>• <b>hmac-md5-96</b>—Produces a 128-bit digest.</li><li>• <b>hmac-sha1-96</b>—Produces a 160-bit digest.</li><li>• <b>hmac-sha-256-128</b>—Produces a 256-bit digest, truncated to 128 bits.</li></ul> <hr/> <div> <b>NOTE:</b> <b>hmac-sha-256-128</b> is not supported on MS-MIC and MS-MPC.</div> <hr/> <p><b>key</b>—Type of authentication key. The key can be one of the following:</p> <ul style="list-style-type: none"><li>• <b>ascii-text key</b>—ASCII text key. For <b>hmac-md5-96</b>, the key is 16 ASCII characters; for <b>hmac-sha1-96</b>, the key is 20 ASCII characters.</li><li>• <b>hexadecimal key</b>—Hexadecimal key. For <b>hmac-md5-96</b>, the key is 32 hexadecimal characters; for <b>hmac-sha1-96</b>, the key is 40 hexadecimal characters.</li></ul>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Security Associations</i></li></ul>

## authentication-algorithm

---

See the following sections:

- [authentication-algorithm \(Services IKE\) on page 539](#)
- [authentication-algorithm \(Services IPsec\) on page 540](#)

### authentication-algorithm (Services IKE)

<b>Syntax</b>	<code>authentication-algorithm (md5   sha1   sha-256);</code>
<b>Hierarchy Level</b>	[ <a href="#">edit services ipsec-vpn ike proposal proposal-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. sha-256 option added in Junos OS Release 7.6.
<b>Description</b>	Configure the Internet Key Exchange (IKE) hash algorithm that authenticates packet data.
<b>Options</b>	<b>md5</b> —Produces a 128-bit digest.  <b>sha1</b> —Produces a 160-bit digest.  <b>sha-256</b> —Produces a 256-bit digest.  <b>sha-384</b> —Produces a 384-bit digest.
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IKE Proposals</i></li></ul>

### authentication-algorithm (Services IPsec)

<b>Syntax</b>	authentication-algorithm (hmac-md5-96   hmac-sha-256-128   hmac-sha1-96);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ipsec proposal</a> <i>ipsec-proposal-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the IPsec hash algorithm that authenticates packet data.
<b>Options</b>	<b>hmac-md5-96</b> —Produces a 128-bit digest. <b>hmac-sha-256-128</b> —Produces a 256-bit digest. <b>hmac-sha1-96</b> —Produces a 160-bit digest.
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Proposals</i></li></ul>

---

### authentication-method (Services IPsec VPN)

<b>Syntax</b>	authentication-method ( pre-shared-keys   rsa-signatures);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ike proposal</a> <i>proposal-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure an IKE authentication method.
<b>Options</b>	<b>rsa-signatures</b> —Public key algorithm (supports encryption and digital signatures). <b>pre-shared-keys</b> —A key derived from an out-of-band mechanism; the key authenticates the exchange.
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IKE Proposals</i></li></ul>

## auxiliary-spi (Services IPsec VPN)

<b>Syntax</b>	<code>auxiliary-spi spi-value;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> rule-name <a href="#">term</a> term-name <a href="#">then</a> manual direction direction]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure an auxiliary Security Parameter Index (SPI) for a manual SA. Use the auxiliary SPI when you configure the <b>protocol</b> statement to use the <b>bundle</b> option.
<b>Options</b>	<p><b>spi-value</b>—An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).</p> <p><b>Range:</b> 256 through 16,639</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Security Associations</i></li> </ul>

## backup-remote-gateway

<b>Syntax</b>	<code>backup-remote-gateway address;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> rule-name <a href="#">term</a> term-name <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the backup remote address to which the IPsec traffic is directed when the primary remote gateway is down. Configuring this statement also enables the dead peer detection (DPD) protocol.
<b>Options</b>	<b>address</b> —Backup remote IPv4 or IPv6 address.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring IPsec Rules</i></li> </ul>

## clear-dont-fragment-bit (Services IPsec VPN)

---

<b>Syntax</b>	clear-dont-fragment-bit;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Clear the do not fragment (DF) bit on all IP version 4 (IPv4) packets entering the IPsec tunnel. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Rules</i></li></ul>

## clear-ike-sas-on-pic-restart

---

<b>Syntax</b>	clear-ike-sas-on-pic-restart;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Clear IKE security associations (SAs) when the corresponding PIC restarts or is taken offline.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Security Associations</i></li></ul>

## clear-ipsec-sas-on-pic-restart

<b>Syntax</b>	clear-ipsec-sas-on-pic-restart;
<b>Hierarchy Level</b>	[edit services ipsec-vpn]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Clear IPsec security associations (SAs) when the corresponding PIC restarts or is taken offline.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Security Associations</i></li> </ul>

## copy-dont-fragment-bit (Services IPsec VPN)

<b>Syntax</b>	copy-dont-fragment-bit;
<b>Hierarchy Level</b>	[edit <b>services</b> ipsec-vpn <b>rule</b> <i>rule-name</i> <b>term</b> <i>term-name</i> <b>then</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Copy the do not fragment (DF) bit value to only the outer header and not modify the inner header of the IPsec packet. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs. These settings apply for static endpoint tunnels and not for dynamic tunnels, for which you need to include the <b>copy-dont-fragment-bit</b> statement at the [edit <b>services service-set</b> <b>service-set-name</b> ipsec-vpn-options] hierarchy level to copy the DF bit value to only the outer header of the packet in a static IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring IPsec Rules</i></li> </ul>

## description (Services IPsec VPN)

---

<b>Syntax</b>	<code>description <i>description</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn ike <a href="#">policy</a> <i>policy-name</i> ], [edit <a href="#">services</a> ipsec-vpn ike <a href="#">proposal</a> <i>proposal-name</i> ], [edit <a href="#">services</a> ipsec-vpn ipsec (Services IPsec VPN) <a href="#">policy</a> <i>policy-name</i> ], [edit <a href="#">services</a> ipsec-vpn ipsec (Services IPsec VPN) <a href="#">proposal</a> <i>proposal-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the text description for an IKE or IPsec policy or proposal.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">description on page 544</a></li><li>• <i>Configuring IPsec Proposals</i></li><li>• <i>Configuring IPsec Policies</i></li></ul>

## destination-address (Services IPsec VPN)

---

<b>Syntax</b>	<code>destination-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the destination address for rule matching.
<b>Options</b>	<i>address</i> —Destination IP address.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Rules</i></li></ul>

## dh-group

---

<b>Syntax</b>	dh-group (group1   group2   group5  group14   group19   group20);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn ike <a href="#">proposal</a> <i>proposal-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the IKE Diffie-Hellman prime modulus group to use for performing the new Diffie-Hellman exchange.
<b>Options</b>	<p><b>group1</b>—768-bit.</p> <p><b>group2</b>—1024-bit.</p> <p><b>group5</b>—1536-bit.</p> <p><b>group14</b>—2048-bit.</p> <p><b>group19</b>—256-bit random Elliptic Curve Group.</p> <p><b>group20</b>—384-bit random Elliptic Curve Group.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IKE Proposals</i></li></ul>

## direction

---

<b>Syntax</b>	<pre>direction (inbound   outbound   bidirectional) {   protocol (ah   bundle   esp);   spi spi-value;   auxiliary-spi spi-value;   authentication (Services IPsec VPN) {     algorithm (hmac-md5-96   hmac-sha1-96);     key (ascii-text key   hexadecimal key);   }   encryption {     algorithm algorithm;     key (ascii-text key   hexadecimal key);   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> rule-name <a href="#">term</a> term-name <a href="#">then manual</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the direction in which manual SAs are applied.
<b>Options</b>	<p><b>bidirectional</b>—Apply the SA in both directions.</p> <p><b>inbound</b>—Apply the SA on inbound traffic.</p> <p><b>outbound</b>—Apply the SA on outbound traffic.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Rules</i></li></ul>

## dynamic

---

<b>Syntax</b>	<pre>dynamic {     ike-policy <i>policy-name</i>;     ipsec-policy <i>policy-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services (IPsec VPN)</a> ipsec-vpn <a href="#">rule (Services IPsec VPN)</a> <i>rule-name</i> <a href="#">term (Services IPsec VPN)</a> <i>term-name</i> <a href="#">then (Services IPsec VPN)</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define a dynamic IPsec SA.
<b>Options</b>	<p><b>ike-policy <i>policy-name</i></b>—Name of the IKE policy. This statement is optional for the non-preshared-key authentication method. For digital signature-based authentication, this statement is optional and the default policy is used if none is supplied.</p> <p><b>ipsec-policy <i>policy-name</i></b>—Name of the IPsec policy. This statement is optional and the default policy is used if none is supplied.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Security Associations</i></li></ul>

## encryption

<b>Syntax</b>	<pre> encryption {     algorithm <i>algorithm</i>;     key (ascii-text <i>key</i>   hexadecimal <i>key</i>); } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> <a href="#">manual</a> direction <i>direction</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <a href="#">aes-128-cbc</a> , <a href="#">aes-192-cbc</a> , and <a href="#">aes-256-cbc</a> options added in Junos OS Release 7.6.
<b>Description</b>	Configure an encryption algorithm and key for manual SA.

**Options** **algorithm**—Type of encryption algorithm. The algorithm can be one of the following:

- **des-cbc**—Has a block size of 8 bytes (64 bits); the key size is 48 bits long.
- **3des-cbc**—Has a block size of 8 bytes (64 bits); the key size is 192 bits long.
- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.



**NOTE:** For **3des-cbc**, the first 8 bytes should differ from the second 8 bytes, and the second 8 bytes should be the same as the third 8 bytes.

**key**—Type of encryption key. The key can be one of the following:

- **ascii-text**—ASCII text key. Following are the key lengths, in ASCII characters, for the different encryption options:
  - **des-cbc** option, 8 ASCII characters
  - **3des-cbc** option, 24 ASCII characters
  - **aes-128-cbc** option, 16 ASCII characters
  - **aes-192-cbc** option, 24 ASCII characters
  - **aes-256-cbc** option, 32 ASCII characters
- **hexadecimal**—Hexadecimal key. Following are the key lengths, in hexadecimal characters, for the different encryption options:
  - **des-cbc** option, 16 hexadecimal characters
  - **3des-cbc** option, 48 hexadecimal characters
  - **aes-128-cbc** option, 32 hexadecimal characters
  - **aes-192-cbc** option, 48 hexadecimal characters

- **aes-256-cbc** option, 64 hexadecimal characters

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Security Associations</i></li> </ul>

## encryption-algorithm (Services IPsec VPN)

<b>Syntax</b>	encryption-algorithm (3des-cbc   aes-128-cbc   aes-192-cbc   aes-256-cbc   des-cbc);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ike proposal</a> <i>proposal-name</i> ], [edit <a href="#">services</a> ipsec-vpn <a href="#">ipsec proposal</a> <i>proposal-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>aes-128-cbc</b> , <b>aes-192-cbc</b> , and <b>aes-256-cbc</b> options added in Junos OS Release 7.6.
<b>Description</b>	Configure an IKE or IPsec encryption algorithm.
<b>Options</b>	<p><b>3des-cbc</b>—Has a block size of 24 bytes; the key size is 192 bits long.</p> <p><b>des-cbc</b>—Has a block size of 8 bytes; the key size is 48 bits long.</p> <p><b>aes-128-cbc</b>—Advanced Encryption Standard (AES) 128-bit encryption algorithm.</p> <p><b>aes-192-cbc</b>—Advanced Encryption Standard (AES) 192-bit encryption algorithm.</p> <p><b>aes-256-cbc</b>—Advanced Encryption Standard (AES) 256-bit encryption algorithm.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Security Associations</i></li> </ul>

## from (Services IPsec VPN)

---

<b>Syntax</b>	from { <code>destination-address</code> <i>address</i> ; <code>ipsec-inside-interface</code> <i>interface-name</i> ; <code>source-address</code> <i>address</i> ; }
<b>Hierarchy Level</b>	[edit <code>services</code> ipsec-vpn <code>rule</code> <i>rule-name</i> <code>term</code> <i>term-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify input conditions for the IPsec term.
<b>Options</b>	<p>For information on match conditions, see the description of firewall filter match conditions in the <i>Junos OS Routing Policy Configuration Guide</i>..</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Rules</i></li></ul>

## ike

```

Syntax  ike {
        proposal proposal-name {
            authentication-algorithm (md5 | sha1 | sha-256);
            authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
            description description;
            dh-group (group1 | group2 | group5 | group14);
            encryption-algorithm algorithm;
            lifetime-seconds seconds;
        }
        policy policy-name {
            description description;
            local-certificate identifier;
            local-id (ipv4_addr ipv4-address | ipv6_addr ipv6-address | key-id identifier);
            version (1 | 2);
            mode (aggressive | main);
            pre-shared-key (ascii-text key | hexadecimal key);
            proposals [ proposal-names ];
            remote-id {
                any-remote-id;
                ipv4_addr [ values ];
                ipv6_addr [ values ];
                key_id [ values ];
            }
        }
    }

```

Hierarchy Level [edit [services](#) ipsec-vpn]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure IKE.

The statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring IKE Proposals*
- *Configuring IKE Policies*

## initiate-dead-peer-detection

---

<b>Syntax</b>	initiate-dead-peer-detection;
<b>Hierarchy Level</b>	[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable triggering of dead peer detection (DPD) hello messages to the remote peer for the specified tunnel.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Rules</i></li><li>• <i>dead-peer-detection</i></li><li>• <a href="#">backup-remote-gateway on page 541</a></li><li>• <a href="#">Configuring Destination Addresses for Dead Peer Detection on page 509</a></li></ul>

## ipsec (Services IPsec VPN)

<b>Syntax</b>	<pre> ipsec {   proposal <i>proposal-name</i> {     authentication-algorithm (hmac-md5-96   hmac-sha1-96);     description <i>description</i>;     encryption-algorithm <i>algorithm</i>;     lifetime-seconds <i>seconds</i>;     protocol (ah   esp   bundle);   }   policy <i>policy-name</i> {     description <i>description</i>;     perfect-forward-secrecy {       keys (group1   group2);     }     proposals [ <i>proposal-names</i> ];   } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Configure IPsec.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Security Associations</i></li> </ul>

## ipsec-inside-interface

<b>Syntax</b>	ipsec-inside-interface <i>interface-name</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Specify the interface name for next-hop-style service sets. This value is also implicitly generated in dynamic endpoint tunneling.
<b>Options</b>	<i>interface-name</i> —Service interface for internal network.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring IPsec Rules</i></li> <li>• <i>Configuring Dynamic Endpoints for IPsec Tunnels</i></li> </ul>

## lifetime-seconds (Services IPsec VPN)

---

<b>Syntax</b>	<code>lifetime-seconds <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ike proposal</a> <i>proposal-name</i> ], [edit <a href="#">services</a> ipsec-vpn <a href="#">ipsec proposal</a> <i>proposal-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the lifetime of an IKE or IPsec SA. This statement is optional.
<b>Options</b>	<b><i>seconds</i></b> —Lifetime <b>Default:</b> 3600 seconds (IKE); 28,800 seconds (IPsec) <b>Range:</b> 180 through 86,400
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Security Associations</i></li></ul>

## local-certificate (Services IPsec VPN)

---

<b>Syntax</b>	<code>local-certificate <i>identifier</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ike policy</a> <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.5.
<b>Description</b>	Name of the certificate that needs to be sent to the peer during the IKE authentication phase.
<b>Options</b>	<b><i>identifier</i></b> —Name of certificate.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IKE Policies</i></li></ul>

## local-id

---

<b>Syntax</b>	<code>local-id (ipv4_addr <i>ipv4-address</i>   ipv6_addr <i>ipv6-address</i>   key-id <i>identifier</i>);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ike</a> <a href="#">policy</a> <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <code>ipv6_addr</code> option added in Junos OS Release 7.6.
<b>Description</b>	Specify local identifiers for IKE Phase 1 negotiation. This statement is optional.
<b>Options</b>	<p><code>ipv4_addr <i>ipv4-address</i></code>—IPv4 address identification value.</p> <p><code>ipv6_addr <i>ipv6-address</i></code>—IPv6 address identification value.</p> <p><code>key_id <i>identifier</i></code>—Key identification value.</p> <p><code>fqdn <i>fqdn</i></code>—Fully-qualified domain name.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring Security Associations</i></li> </ul>

## manual

---

Syntax	<pre>manual {   direction (inbound   outbound   bidirectional) {     authentication {       algorithm (hmac-md5-96   hmac-sha1-96);       key (ascii-text key   hexadecimal key);     }     auxiliary-spi spi-value;     encryption {       algorithm algorithm;       key (ascii-text key   hexadecimal key);     }     spi spi-value;     protocol (ah   esp   bundle);   } }</pre>
Hierarchy Level	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> rule-name <a href="#">term</a> term-name <a href="#">then</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define a manual IPsec SA.  The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring Security Associations</i></li></ul>

## match-direction (Services IPsec VPN)

---

Syntax	<pre>match-direction (input   output);</pre>
Hierarchy Level	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> rule-name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the direction in which the rule match is applied.
Options	<b>input</b> —Apply the rule match on input.  <b>output</b> —Apply the rule match on output.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Rules</i></li></ul>

## mode (Services IPsec VPN)

<b>Syntax</b>	mode (aggressive   main);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ike</a> <a href="#">policy</a> <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define an IKE policy mode.
<b>Default</b>	main
<b>Options</b>	<p><b>aggressive</b>—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection.</p> <p><b>main</b>—Uses six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring IKE Policies</i></li> </ul>

## no-anti-replay (Services IPsec VPN)

<b>Syntax</b>	no-anti-replay;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Disable IPsec antireplay service, which occasionally causes interoperability issues for security associations.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Security Associations</i></li> </ul>

## no-ipsec-tunnel-in-traceroute

---

<b>Syntax</b>	no-ipsec-tunnel-in-traceroute;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Disables displaying the IPsec tunnel endpoint in the trace route output. The IPsec tunnel is not treated as a next hop and TTL is not decremented. If the TTL becomes zero, the ICMP time exceeded message will not be generated.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Security Associations</i></li></ul>

## perfect-forward-secrecy (Services IPsec VPN)

---

<b>Syntax</b>	perfect-forward-secrecy { keys (group1   group2   group5   group14   group19   group20); }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ipsec policy</a> <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define Perfect Forward Secrecy (PFS). Creates single-use keys. This statement is optional.
<b>Options</b>	<b>keys</b> —Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange. The key can be one of the following: <ul style="list-style-type: none"><li>• <b>group1</b>—768-bit.</li><li>• <b>group2</b>—1024-bit.</li><li>• <b>group5</b>—1536-bit.</li><li>• <b>group14</b>—2048-bit.</li><li>• <b>group19</b>—256-bit random Elliptic Curve Group.</li><li>• <b>group20</b>—384-bit random Elliptic Curve Group.</li></ul>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Security Associations</i></li></ul>

## policy

---

See the following sections:

- [policy \(Services IKE\) on page 559](#)
- [policy \(Services IPsec VPN\) on page 560](#)

### policy (Services IKE)

**Syntax** `policy policy-name {  
     description description;  
     local-certificate identifier;  
     local-id (ipv4_addr ipv4-address | ipv6_addr ipv6-address | key-id identifier);  
     version (1 | 2);  
     mode (aggressive | main);  
     pre-shared-key (ascii-text key | hexadecimal key);  
     proposals [ proposal-names ];  
     remote-id {  
         any-remote-id;  
         ipv4_addr [ values ];  
         ipv6_addr [ values ];  
         key_id [ values ];  
     }  
 }`

**Hierarchy Level** [edit [services](#) ipsec-vpn [ike](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define an IKE policy.

**Options** *policy-name*—IKE policy name.

The remaining statements are explained separately.

**Required Privilege Level** admin—To view this statement in the configuration.  
 admin-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring IKE Policies](#)

## policy (Services IPsec VPN)

<b>Syntax</b>	<pre>policy <i>policy-name</i> {   <b>description</b> <i>description</i>;   <b>perfect-forward-secrecy</b> {     keys (group1   group 14   group2   group 5);   }   <b>proposals</b> [ <i>proposal-names</i> ]; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ipsec</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define an IPsec policy.
<b>Options</b>	<p><i>policy-name</i>—IPsec policy name.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Policies</i></li></ul>

---

## pre-shared-key (Services IKE)

<b>Syntax</b>	<pre>pre-shared-key (ascii-text <i>key</i>   hexadecimal <i>key</i>);</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">ike</a> <a href="#">policy</a> <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define a preshared key for an IKE policy.
<b>Options</b>	<p><i>key</i>—Value of preshared key. The key can be one of the following:</p> <ul style="list-style-type: none"><li>• <b>ascii-text</b>—ASCII text key.</li><li>• <b>hexadecimal</b>—Hexadecimal key.</li></ul>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IKE Policies</i></li></ul>

## proposal

---

See the following sections:

- [proposal \(Services IKE\)](#) on page 561
- [proposal \(Services IPsec VPN\)](#) on page 562

### proposal (Services IKE)

**Syntax**    `proposal proposal-name {  
                   authentication-algorithm (md5 | sha1 | sha-256);  
                   authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);  
                   description description;  
                   dh-group (group1 | group2 | group5 | group14);  
                   encryption-algorithm algorithm;  
                   lifetime-seconds seconds;  
                   }`

**Hierarchy Level**    [edit [services](#) ipsec-vpn [ike](#)]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Define an IKE proposal for a dynamic SA.

**Options**    *proposal-name*—IKE proposal name.

The remaining statements are explained separately.

**Required Privilege Level**    system—To view this statement in the configuration.  
    system-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring IKE Proposals](#)

## proposal (Services IPsec VPN)

Syntax	<pre>proposal <i>proposal-name</i> {   authentication-algorithm (hmac-md5-96   hmac-sha1-96);   description <i>description</i>;   encryption-algorithm <i>algorithm</i>;   lifetime-seconds <i>seconds</i>;   protocol (ah   esp   bundle); }</pre>
Hierarchy Level	[edit <a href="#">services</a> ipsec-vpn <a href="#">ipsec</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define an IPsec proposal for a dynamic SA.
Options	<p><i>proposal-name</i>—IPsec proposal name.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Proposals</i></li></ul>

---

## proposals

Syntax	<pre>proposals [ <i>proposal-names</i> ];</pre>
Hierarchy Level	[edit <a href="#">services</a> ipsec-vpn <a href="#">ike policy</a> <i>policy-name</i> ], [edit <a href="#">services</a> ipsec-vpn <a href="#">ipsec policy</a> <i>policy-name</i> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define a list of proposals to include in the IKE or IPsec policy.
Options	<i>proposal-names</i> —List of IKE or IPsec proposal names.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring IKE Proposals</i></li><li>• <i>Configuring IPsec Proposals</i></li></ul>

## protocol

---

<b>Syntax</b>	<code>protocol (ah   esp   bundle);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ipsec proposal</a> <i>proposal-name</i> ], [edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> manual direction <i>direction</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define an IPsec protocol for a dynamic or manual SA.
<b>Options</b>	<b>ah</b> —Authentication Header protocol.  <b>esp</b> —Encapsulating Security Payload protocol.  <b>bundle</b> —AH and ESP protocol.
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Security Associations</i></li> </ul>

## remote-gateway

---

<b>Syntax</b>	<code>remote-gateway <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the remote address to which the IPsec traffic is directed.
<b>Options</b>	<b><i>address</i></b> —Remote IPv4 or IPv6 address.
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring IPsec Rules</i></li> </ul>

## remote-id

---

<b>Syntax</b>	<pre>remote-id {   any-remote-id;   ipv4_addr [ <i>values</i> ];   ipv6_addr [ <i>values</i> ];   key_id [ <i>values</i> ]; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ikepolicy</a> <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>ipv6_addr</b> option added in Junos OS Release 7.6. <b>any-remote-id</b> option added in Junos OS Release 8.2.
<b>Description</b>	Define the remote identification values to which the IKE policy applies.
<b>Options</b>	<p><b>any-remote-id</b>—Allow any remote address to connect. This option is supported only in dynamic configurations and cannot be configured with specific values.</p> <p><b>ipv4_addr [ <i>values</i> ]</b>—Define one or more IPv4 address identification values.</p> <p><b>ipv6_addr [ <i>values</i> ]</b>—Define one or more IPv6 address identification values.</p> <p><b>key_id [ <i>values</i> ]</b>—Define one or more key identification values.</p> <p><b>fqdn <i>fqdn</i></b>—Fully-qualified domain name.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IKE Policies</i></li></ul>

## rule (Services IPsec VPN)

```
Syntax  rule rule-name {
        match-direction (input | output);
        term term-name {
            from {
                destination-address address;
                ipsec-inside-interface interface-name;
                source-address address;
            }
            then {
                anti-replay-window-size bits;
                backup-remote-gateway address;
                clear-dont-fragment-bit;
                dynamic {
                    ike-policy policy-name;
                    ipsec-policy policy-name;
                }
                initiate-dead-peer-detection;
                manual {
                    direction (inbound | outbound | bidirectional) {
                        authentication {
                            algorithm (hmac-md5-96 | hmac-sha1-96);
                            key (ascii-text key | hexadecimal key);
                        }
                        auxiliary-spi spi-value;
                        encryption {
                            algorithm algorithm;
                            key (ascii-text key | hexadecimal key);
                        }
                        protocol (ah | bundle | esp);
                        spi spi-value;
                    }
                }
                no-anti-replay;
                remote-gateway address;
                syslog;
                tunnel-mtu bytes;
            }
        }
    }
```

**Hierarchy Level** [edit [services](#) ipsec-vpn],  
[edit [services](#) ipsec-vpn [rule-set](#) *rule-set-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Specify the rule the router uses when applying this service.

**Options** *rule-name*—Identifier for the collection of terms that comprise this rule.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring IPsec Rules*
- *Configuring IPsec Rule Sets*
- *Configuring Security Associations*

---

## rule-set (Services IPsec VPN)

---

**Syntax** `rule-set rule-set-name {  
[ rule rule-names ];  
}`

**Hierarchy Level** [edit [services](#) ipsec-vpn]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Specify the rule set the router uses when applying this service.

**Options** *rule-set-name*—Identifier for the collection of rules that constitute this rule set.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring IPsec Rules*

---

## services (IPsec VPN)

---

**Syntax** `services ipsec-vpn { ... }`

**Hierarchy Level** [edit]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the service rules to be applied to traffic.

**Options** *ipsec-vpn*—IPsec set of rules statements.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring Security Associations*

## set-dont-fragment-bit (Services IPsec VPN)


<b>Syntax</b>	set-dont-fragment-bit;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Configure the do not fragment (DF) bit in only the outer header of the IPsec packet and leave the inner header unmodified. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. These settings apply for static endpoint tunnels and not for dynamic tunnels, for which you need to include the <b>set-dont-fragment-bit</b> statement at the [edit <a href="#">services</a> <a href="#">service-set</a> <a href="#">service-set-name</a> ipsec-vpn-options] hierarchy level to set the DF bit in the outer header of the IPv4 packets that enter the dynamic IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring IPsec Rules</i></li> </ul>

## source-address (Services IPsec VPN)

<b>Syntax</b>	source-address <i>address</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the source address for rule matching.
<b>Options</b>	<i>address</i> —Source IP address.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring IPsec Rules</i></li> </ul>

## spi

---

<b>Syntax</b>	<code>spi spi-value;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> manual direction <i>direction</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the SPI for an SA.
<b>Options</b>	<b>spi-value</b> —An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet). <b>Range:</b> 256 through 16,639
<hr/>	
<div> <b>NOTE:</b> Use the auxiliary SPI when you configure the protocol statement to use the <b>bundle</b> option.</div> <hr/>	
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Security Associations</i></li></ul>

## syslog (Services IPsec VPN)

---

<b>Syntax</b>	<code>syslog;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Enable system logging. The system log information for the Adaptive Services or Multiservices Physical Interface Card (PIC) is passed to the kernel for logging in the <code>/var/log</code> directory.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring IPsec Rules</i></li></ul>

## term (Services IPsec VPN)

```
Syntax  term term-name {
        from {
            destination-address address;
            ipsec-inside-interface interface-name;
            source-address address;
        }
        then {
            anti-replay-window-size bits;
            backup-remote-gateway address;
            clear-dont-fragment-bit;
            dynamic {
                ike-policy policy-name;
                ipsec-policy policy-name;
            }
            initiate-dead-peer-detection;
            manual {
                direction (inbound | outbound | bidirectional) {
                    authentication {
                        algorithm (hmac-md5-96 | hmac-sha1-96);
                        key (ascii-text key | hexadecimal key);
                    }
                    auxiliary-spi spi-value;
                    encryption {
                        algorithm algorithm;
                        key (ascii-text key | hexadecimal key);
                    }
                    protocol (ah | bundle | esp);
                    spi spi-value;
                }
            }
            no-anti-replay;
            remote-gateway address;
            syslog;
            tunnel-mtu bytes;
        }
    }
```

**Hierarchy Level** [edit [services](#) ipsec-vpn [rule](#) *rule-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the IPsec term properties.

**Options** *term-name*—Identifier for the term.

The remaining statements are explained separately.

**Required Privilege** interface—To view this statement in the configuration.

**Level** interface-control—To add this statement to the configuration.

Related Documentation • [Configuring IPsec Rules](#)

## then (Services IPsec VPN)

```
Syntax  then {
        anti-replay-window-size bits;
        backup-remote-gateway address;
        clear-dont-fragment-bit;
        dynamic {
            ike-policy policy-name;
            ipsec-policy policy-name;
        }
        initiate-dead-peer-detection;
        dead-peer-detection {
            interval seconds;
            threshold number;
        }
        manual {
            direction (inbound | outbound | bidirectional) {
                authentication {
                    algorithm (hmac-md5-96 | hmac-sha1-96);
                    key (ascii-text key | hexadecimal key);
                }
                auxiliary-spi spi-value;
                encryption {
                    algorithm algorithm;
                    key (ascii-text key | hexadecimal key);
                }
                protocol (ah | bundle | esp);
                spi spi-value;
            }
        }
        no-anti-replay;
        remote-gateway address;
        syslog;
        tunnel-mtu bytes;
    }
```

Hierarchy Level [edit [services](#) ipsec-vpn [rule](#) *rule-name* [term](#) *term-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the IPsec term actions.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

Related Documentation • [Configuring IPsec Rules](#)

## traceoptions (Services IPsec VPN)

<b>Syntax</b>	<pre> traceoptions {     file &lt;filename&gt; &lt;files number&gt; &lt;match regular-expression&gt; &lt;size bytes&gt; &lt;world-readable           no-world-readable&gt;;     flag flag;     level level;     no-remote-trace; } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.5. level option added in Junos OS Release 10.0.
<b>Description</b>	Configure IPsec tracing operations. By default, messages are written to <code>/var/log/kmd</code> .
<b>Options</b>	<p><b>files <i>number</i></b>—Maximum number of trace data files.  <b>Range:</b> 2 through 1000</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace everything.</li> <li>• <b>certificates</b>—Trace certificates that apply to the IPsec service set.</li> <li>• <b>database</b>—Trace security associations database events.</li> <li>• <b>general</b>—Trace general events.</li> <li>• <b>ike</b>—Trace IKE module processing.</li> <li>• <b>parse</b>—Trace configuration processing.</li> <li>• <b>policy-manager</b>—Trace policy manager processing.</li> <li>• <b>routing-socket</b>—Trace routing socket messages.</li> <li>• <b>snmp</b>—Trace SNMP operations.</li> <li>• <b>timer</b>—Trace internal timer events.</li> </ul> <p><b>level <i>level</i></b>—Key management process (kmd) tracing level. The following values are supported:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Match all levels.</li> <li>• <b>error</b>—Match error conditions.</li> <li>• <b>info</b>—Match informational messages.</li> <li>• <b>notice</b>—Match conditions that should be handled specially.</li> <li>• <b>verbose</b>—Match verbose messages.</li> <li>• <b>warning</b>—Match warning messages.</li> </ul>

**size bytes**—Maximum trace file size.

<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Tracing Junos VPN Site Secure Operations</i></li></ul>
------------------------------	---

## traceoptions (PKI)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i>&gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>; } </pre>
<b>Hierarchy Level</b>	[edit security pki]
<b>Description</b>	Configure security public key infrastructure (PKI) trace options. To specify more than one trace option, include multiple <b>flag</b> statements. Trace option output is recorded in the <code>/var/log/pkid</code> file.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. To include the <b>file</b> statement, you must specify a filename.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file (for example, <b>pkid</b>) reaches its maximum size, it is renamed <b>pkid.0</b>, then <b>pkid.1</b>, and so on, until the maximum number of trace files is reached. When the maximum number is reached, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 2 files</p> <p><b>flag</b>—Trace operation to perform. To specify more than one trace operation, include multiple flag statements:</p> <ul style="list-style-type: none"> <li><b>all</b>—Trace with all flags enabled.</li> <li><b>certificate-verification</b>—Trace PKI certificate verification events.</li> <li><b>online-crl-check</b>—Trace PKI online certificate revocation list (CRL) events.</li> <li><b>enrollment</b>—PKI certificate enrollment tracing.</li> </ul> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p><b>size <i>maximum-file-size</i></b>—(Optional) Maximum size of each trace file, in kilobytes (KB). If you specify a maximum file size, you also must specify a maximum number of trace files with the <b>files <i>number</i></b> option.</p> <p><b>Default:</b> 1024 KB</p> <p><b>world-readable   no-world-readable</b>—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The <b>world-readable</b> option enables any user to read the file. To explicitly set the default behavior, use the <b>no-world-readable</b> option.</p>

**Required Privilege Level** trace—To view this statement in the configuration.  
trace-control—To add this statement to the configuration.

**Related Documentation**

- *Tracing Junos VPN Site Secure Operations*

---

## tunnel-mtu (Services IPsec VPN)

---

**Syntax** tunnel-mtu *bytes*;

**Hierarchy Level** [edit [services](#) ipsec-vpn [rule](#) *rule-name* [term](#) *term-name* [then](#)]

**Release Information** Statement introduced in Junos OS Release 7.5.

**Description** Maximum transmission unit (MTU) size for IPsec tunnels.

**Options** *bytes*—MTU size.  
**Default:** 1500 bytes  
**Range:** 256 through 9192 bytes



**NOTE:** Clear the IPsec SA in tunnel-mtu to accomodate Jumbo frames larger than 1500 bytes.

---


**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Specifying the MTU for IPsec Tunnels on page 511](#)
- [mtu on page 1456](#)

## version (IKE)

---

<b>Syntax</b>	version ( 1   2 );
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ipsec-vpn <a href="#">ike policy</a> <i>policy-name</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Configure the Internet Key Exchange (IKE) version that is used to negotiate dynamic SAs for IPsec.
<b>Options</b>	1—Uses IKEv1. 2—Uses IKEv2.
<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p><b>NOTE:</b> By default, Junos OS uses IKE policy version 1.0. Version 2.0 is supported only in Junos OS Release 11.4 and later. If no version is explicitly configured, Junos OS sets the version to version 1.0.</p> </div> </div>	
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring IKE Policies</i></li> </ul>



## CHAPTER 21

# Layer 2 Tunneling Protocol Services Configuration Guidelines

The Layer 2 Tunneling Protocol (L2TP) enables you to set up client services for establishing Point-to-Point Protocol (PPP) tunnels across a network and negotiating Multilink PPP if it is implemented. Multiple L2TP PPP sessions can share the same remote peer IP address, which enables you to set up redundant sessions between the same links.

- If you configure Multilink PPP, the same remote IP address can be shared across multiple bundles, because the IP address negotiation takes place on the bundle rather than on each session.
- If Multilink PPP is not configured, multiple sessions can share the same remote IP address.

The last session or bundle to come up accomplishes the traffic transfer. When this session or bundle goes down, the traffic switches to the next-to-last session or bundle to come up. For example, if four sessions or bundles labeled A, B, C, and D share the same remote IP address and come up in alphabetical order, D initially handles the data transfer. If D goes down, traffic switches over to C, and so forth. If another session or bundle E subsequently comes up and has the same address, the traffic switches over to it.

To configure L2TP services, include the **l2tp** statement at the **[edit services]** hierarchy level:

```
[edit services]
l2tp {
  ip-reassembly;
  tunnel-group group-name {
    hello-interval seconds;
    hide-avps;
    l2tp-access-profile profile-name;
    local-gateway address;
    maximum-send-window packets;
    ppp-access-profile profile-name;
    receive-window packets;
    retransmit-interval seconds;
    service-interface interface-name;
    syslog {
      host hostname {
        services severity-level;
```

```

        facility-override facility-name;
        log-prefix prefix-value;
    }
}
tunnel-timeout seconds;
}
traceoptions {
    debug-level level;
    filter {
        protocol name;
    }
    flag flag;
    interfaces interface-name {
        debug-level level;
        flag flag;
    }
}
}

```



**NOTE:** L2TP configurations on Adaptive Services and Multiservices PICs are supported only on M7i, M10i, and M120 routers. For information about L2TP LAC and LNS configurations on MX Series routers for subscriber access, see *L2TP for Subscriber Access Overview* in the *Junos Subscriber Access Configuration Guide*.

You configure other components of this feature at the **[edit access]** and **[edit interfaces]** hierarchy levels. Those configurations are summarized in this chapter; for more information, see the *Junos OS Administration Library for Routing Devices* or the *Junos OS Network Interfaces Library for Routing Devices*.

This chapter contains the following sections:

- [L2TP Services Configuration Overview on page 579](#)
- [L2TP Minimum Configuration on page 580](#)
- [Configuring L2TP Tunnel Groups on page 582](#)
- [Configuring the Identifier for Logical Interfaces that Provide L2TP Services on page 587](#)
- [AS PIC Redundancy for L2TP Services on page 589](#)
- [IP Packet Fragment Reassembly for L2TP Overview on page 589](#)
- [Configuring IP Inline Reassembly for L2TP on page 590](#)
- [Tracing L2TP Operations on page 591](#)
- [Examples: Configuring L2TP Services on page 593](#)

## L2TP Services Configuration Overview

The statements for configuring L2TP services are found at the following hierarchy levels:

- **[edit services l2tp tunnel-group *group-name*]**

The L2TP **tunnel-group** statement identifies an L2TP instance or L2TP server. Associated statements specify the local gateway address on which incoming tunnels and sessions are accepted, the Adaptive Services (AS) Physical Interface Card (PIC) that processes data for the sessions in this tunnel group, references to L2TP and PPP access profiles, and other attributes for configuring window sizes and timer values.

- **[edit interfaces *sp-fpc/pic/port* unit *logical-unit-number* dial-options]**

The **dial-options** statement includes configuration for the **l2tp-interface-id** statement and the **shared/dedicated** flag. The interface identifier associates a user session with a logical interface. Sessions can use either shared or dedicated logical interfaces. To run routing protocols, a session must use a dedicated logical interface.

- **[edit access profile *profile-name* client *name* l2tp]**

Tunnel profiles are defined at the **[edit access]** hierarchy level. Tunnel clients are defined with authentication, multilink negotiation and fragmentation, and other L2TP attributes in these profiles.

- **[edit access profile *profile-name* client *name* ppp]**

User profiles are defined at the **[edit access]** hierarchy level. User clients are defined with authentication and other PPP attributes in these profiles. These client profiles are used when local authentication is specified.

- **[edit access radius-server *address*]**

When you configure **authentication-order radius** at the **[edit access profile *profile-name*]** hierarchy level, you must configure a RADIUS service at the **[edit access radius-server]** hierarchy level.



**NOTE:** For information about L2TP LAC and LNS configurations on MX Series routers for subscriber access, see *L2TP for Subscriber Access Overview*.

### Related Documentation

- [Layer 2 Tunneling Protocol Overview on page 78](#)
- [AS PIC Redundancy for L2TP Services on page 589](#)
- [L2TP Minimum Configuration on page 580](#)
- [Examples: Configuring L2TP Services on page 593](#)

## L2TP Minimum Configuration

---

To configure L2TP services, you must perform at least the following tasks:

- Define a tunnel group at the **[edit services l2tp]** hierarchy level with the following attributes:
  - **l2tp-access-profile**—Profile name for the L2TP tunnel.
  - **ppp-access-profile**—Profile name for the L2TP user.
  - **local-gateway**—Address for the L2TP tunnel.
  - **service-interface**—AS PIC interface for the L2TP service.
  - Optionally, you can configure **traceoptions** for debugging purposes.

The following example shows a minimum configuration for a tunnel group with trace options:

```
[edit services l2tp]
tunnel-group finance-lns-server {
  l2tp-access-profile westcoast_bldg_1_tunnel;
  ppp-access-profile westcoast_bldg_1;
  local-gateway {
    address 10.21.255.129;
  }
  service-interface sp-1/3/0;
}
traceoptions {
  flag all;
  filter {
    protocol udp;
    protocol l2tp;
    protocol ppp;
    protocol radius;
  }
}
```

- At the **[edit interfaces]** hierarchy level:
  - Identify the physical interface at which L2TP tunnel packets enter the router, for example **ge-0/3/0**.
  - Configure the AS PIC interface with **unit 0 family inet** defined for IP service, and configure another logical interface with **family inet** and the **dial-options** statement.

The following example shows a minimum interfaces configuration for L2TP:

```
[edit interfaces]
ge-0/3/0 {
  unit 0 {
    family inet {
      address 10.58.255.129/28;
    }
  }
}
```

```

sp-1/3/0 {
  unit 0 {
    family inet;
  }
  unit 20 {
    dial-options {
      l2tp-interface-id test;
      shared;
    }
    family inet;
  }
}

```

- At the **[edit access]** hierarchy level:
  - Configure a tunnel profile. Each client specifies a unique L2TP Access Concentrator (LAC) name with an **interface-id** value that matches the one configured on the AS PIC interface unit; **shared-secret** is authentication between the LAC and the L2TP Network Server (LNS).
  - Configure a user profile. If RADIUS is used as the authentication method, it needs to be defined.
  - Define the RADIUS server with an IP address, port, and authentication data shared between the router and the RADIUS server.



**NOTE:** When the L2TP Network Server (LNS) is configured with RADIUS authentication, the default behavior is to accept the preferred RADIUS-assigned IP address. Previously, the default behavior was to accept and install the nonzero peer IP address that came into the IP-Address option of the IPCP Configuration Request packet.

- Optionally, you can define a group profile for common attributes, for example **keepalive 0** to turn off keepalive messages.

The following example shows a minimum profiles configuration for L2TP:

```

[edit access]
group-profile westcoast_users {
  ppp {
    keepalive 0;
  }
}
profile westcoast_bldg_1_tunnel {
  client production {
    l2tp {
      interface-id test;
      shared-secret "$9$n8HX6A01RhIvL1R"; # SECRET-DATA
    }
    user-group-profile westcoast_users;
  }
}
profile westcoast_bldg_1 {
  authentication-order radius;
}

```

```
}
radius-server {
  192.168.65.63 {
    port 1812;
    secret "$9$Vyb4ZHkPQ39mf9pORlexNdbgoZUjqP5"; # SECRET-DATA
  }
}
```

**Related  
Documentation**

- [L2TP Services Configuration Overview on page 579](#)
- [Configuring L2TP Tunnel Groups on page 582](#)
- [Configuring the Identifier for Logical Interfaces that Provide L2TP Services on page 587](#)
- [Tracing L2TP Operations on page 591](#)
- [Examples: Configuring L2TP Services on page 593](#)

---

## Configuring L2TP Tunnel Groups

To establish L2TP service on a router, you need to identify an L2TP tunnel group and specify a number of values that define which access profiles, interface addresses, and other properties to use in creating a tunnel. To identify the tunnel group, include the **tunnel-group** statement at the **[edit services l2tp]** hierarchy level:

```
tunnel-group group-name {
  hello-interval seconds;
  hide-avps;
  l2tp-access-profile profile-name;
  local-gateway address {
    address address;
    gateway-name gateway-name;
  }
  maximum-send-window packets;
  ppp-access-profile profile-name;
  receive-window packets;
  retransmit-interval seconds;
  service-interface interface-name;
  syslog {
    host hostname {
      services severity-level;
      facility-override facility-name;
      log-prefix prefix-value;
    }
  }
  tunnel-timeout seconds;
}
```



**NOTE:** If you delete a tunnel group or mark it inactive, all L2TP sessions in that tunnel group are terminated. If you change the value of the `local-gateway` address or the `service-interface` statement, all L2TP sessions using those settings are terminated. If you change or delete other statements at the `[edit services l2tp tunnel-group group-name]` hierarchy level, new tunnels you establish will use the updated values but existing tunnels and sessions are not affected.

The following sections explain how to configure L2TP tunnel groups:

- [Configuring Access Profiles for L2TP Tunnel Groups on page 583](#)
- [Configuring the Local Gateway Address and PIC on page 583](#)
- [Configuring Window Size for L2TP Tunnels on page 584](#)
- [Configuring Timers for L2TP Tunnels on page 584](#)
- [Hiding Attribute-Value Pairs for L2TP Tunnels on page 585](#)
- [Configuring System Logging of L2TP Tunnel Activity on page 585](#)

## Configuring Access Profiles for L2TP Tunnel Groups

To validate L2TP connections and session requests, you set up access profiles by configuring the `profile` statement at the `[edit access]` hierarchy level. You need to configure two types of profiles:

- L2TP tunnel access profile, which validates all L2TP connection requests to the specified local gateway address
- PPP access profile, which validates all PPP session requests through L2TP tunnels established to the local gateway address

For more information on configuring the profiles, see the *Junos OS Administration Library for Routing Devices*. A profile example is included in [“Examples: Configuring L2TP Services” on page 593](#).

To associate the profiles with a tunnel group, include the `l2tp-access-profile` and `ppp-access-profile` statements at the `[edit services l2tp tunnel-group group-name]` hierarchy level:

```
l2tp-access-profile profile-name;
ppp-access-profile profile-name;
```

## Configuring the Local Gateway Address and PIC

When you configure an L2TP group, you must also define a local address for the L2TP tunnel connections and the AS PIC that processes the requests:

- To configure the local gateway IP address, include the `address` statement at the `[edit services l2tp tunnel-group group-name local-gateway]` hierarchy level:  

```
address address;
```

- To configure the AS PIC, include the **service-interface** statement at the **[edit services l2tp tunnel-group group-name]** hierarchy level:

```
service-interface sp-fpc/pic/port;
```

You can optionally specify the logical unit number along with the service interface. If specified, the unit is used as a logical interface representing PPP sessions negotiated using this profile.



**NOTE:** If you change the local gateway address or the service interface configuration, all L2TP sessions using those settings are terminated.

---

Dynamic class-of-service (CoS) functionality is supported on L2TP LNS sessions or L2TP sessions with ATM VCs, as long as the L2TP session is configured to use an IQ2 PIC on the egress interface. For more information, see the *Junos OS Class of Service Library for Routing Devices*.

## Configuring Window Size for L2TP Tunnels

You can configure the maximum window size for packet processing at each end of the L2TP tunnel:

- The receive window size limits the number of concurrent packets the server processes. By default, the maximum is 16 packets. To change the window size, include the **receive-window** statement at the **[edit services l2tp tunnel-group group-name]** hierarchy level:

```
receive-window packets;
```

- The maximum-send window size limits the other end's receive window size. The information is transmitted in the receive window size attribute-value pair. By default, the maximum is 32 packets. To change the window size, include the **maximum-send-window** statement at the **[edit services l2tp tunnel-group group-name]** hierarchy level:

```
maximum-send-window packets;
```

## Configuring Timers for L2TP Tunnels

You can configure the following timer values that regulate L2TP tunnel processing:

- Hello interval—If the server does not receive any messages within a specified time interval, the router software sends a hello message to the tunnel's remote peer. By default, the interval length is 60 seconds. If you configure a value of 0, no hello messages are sent. To configure a different value, include the **hello-interval** statement at the **[edit services l2tp tunnel-group group-name]** hierarchy level:

```
hello-interval seconds;
```

- Retransmit interval—By default, the retransmit interval length is 30 seconds. To configure a different value, include the **retransmit-interval** statement at the **[edit services l2tp tunnel-group group-name]** hierarchy level:

`retransmit-interval seconds;`

- Tunnel timeout—If the server cannot send any data through the tunnel within a specified time interval, it assumes that the connection with the remote peer has been lost and deletes the tunnel. By default, the interval length is 120 seconds. To configure a different value, include the `tunnel-timeout` statement at the `[edit services l2tp tunnel-group group-name]` hierarchy level:

`tunnel-timeout seconds;`

## Hiding Attribute-Value Pairs for L2TP Tunnels

Once an L2TP tunnel has been established and the connection authenticated, information is encoded by means of attribute-value pairs. By default, this information is not hidden. To hide the attribute-value pairs once the shared secret is known, include the `hide-avps` statement at the `[edit services l2tp tunnel-group group-name]` hierarchy level:

`hide-avps;`

## Configuring System Logging of L2TP Tunnel Activity

You can specify properties that control how system log messages are generated for L2TP services.

To configure interface-wide default system logging values, include the `syslog` statement at the `[edit services l2tp tunnel-group group-name]` hierarchy level:

```
syslog {
  host hostname {
    services severity-level;
    facility-override facility-name;
    log-prefix prefix-value;
  }
}
```

Configure the `host` statement with a hostname or IP address that specifies the system log target server. The hostname `local` directs system log messages to the Routing Engine. For external system log servers, the hostname must be reachable from the same routing instance to which the initial data packet (that triggered session establishment) is delivered. You can specify only one system logging hostname.

Table 30 on page 585 lists the severity levels that you can specify in configuration statements at the `[edit services l2tp tunnel-group group-name syslog host hostname]` hierarchy level. The levels from `emergency` through `info` are in order from highest severity (greatest effect on functioning) to lowest.

**Table 30: System Log Message Severity Levels**

Severity Level	Description
<code>any</code>	Includes all severity levels
<code>emergency</code>	System panic or other condition that causes the router to stop functioning

Table 30: System Log Message Severity Levels (*continued*)

Severity Level	Description
<b>alert</b>	Conditions that require immediate correction, such as a corrupted system database
<b>critical</b>	Critical conditions, such as hard drive errors
<b>error</b>	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
<b>warning</b>	Conditions that warrant monitoring
<b>notice</b>	Conditions that are not errors but might warrant special handling
<b>info</b>	Events or nonerror conditions of interest

We recommend setting the system logging severity level to **error** during normal operation. To monitor PIC resource usage, set the level to **warning**. To gather information about an intrusion attack when an intrusion detection system error is detected, set the level to **notice** for a specific service set. To debug a configuration or log Network Address Translation (NAT) events, set the level to **info**.

For more information about system log messages, see the *Junos OS System Log Messages Reference*.

To use one particular facility code for all logging to the specified system log host, include the **facility-override** statement at the **[edit services l2tp tunnel-group group-name syslog host hostname]** hierarchy level:

```
facility-override facility-name;
```

The supported facilities include: **authorization**, **daemon**, **ftp**, **kernel**, **user**, and **local0** through **local7**.

To specify a text prefix for all logging to this system log host, include the **log-prefix** statement at the **[edit services l2tp tunnel-group group-name syslog host hostname]** hierarchy level:

```
log-prefix prefix-text;
```

#### Related Documentation

- [L2TP Services Configuration Overview on page 579](#)
- [L2TP Minimum Configuration on page 580](#)
- [Configuring the Identifier for Logical Interfaces that Provide L2TP Services on page 587](#)
- [Tracing L2TP Operations on page 591](#)
- [Examples: Configuring L2TP Services on page 593](#)

## Configuring the Identifier for Logical Interfaces that Provide L2TP Services

You can configure L2TP services on adaptive services interfaces on M7i, M10i, and M120 routers only. You must configure the logical interface to be dedicated or shared. If a logical interface is dedicated, it can represent only one session at a time. A shared logical interface can have multiple sessions.

To configure the logical interface, include the **l2tp-interface-id** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* dial-options]** hierarchy level:

```
l2tp-interface-id name;  
(dedicated | shared);
```

The **l2tp-interface-id** name configured on the logical interface must be replicated at the **[edit access profile *name*]** hierarchy level:

- For a user-specific identifier, include the **l2tp-interface-id** statement at the **[edit access profile *name* ppp]** hierarchy level.
- For a group identifier, include the **l2tp-interface-id** statement at the **[edit access profile *name* l2tp]** hierarchy level.

You can configure multiple logical interfaces with the same interface identifier, to be used as a pool for several users. For more information on configuring access profiles, see the *Junos OS Administration Library for Routing Devices*.



**NOTE:** If you delete the **dial-options** statement settings configured on a logical interface, all L2TP sessions running on that interface are terminated.

### Example: Configuring Multilink PPP on a Shared Logical Interface

Multilink PPP is supported on either shared or dedicated logical interfaces. The following example can be used to configure many multilink bundles on a single shared interface:

```
interfaces {  
  sp-1/3/0 {  
    traceoptions {  
      flag all;  
    }  
    unit 0 {  
      family inet;  
    }  
    unit 20 {  
      dial-options {  
        l2tp-interface-id test;  
        shared;  
      }  
      family inet;  
    }  
  }  
}
```

```
access {
  profile t {
    client test {
      l2tp {
        interface-id test;
        multilink;
        shared-secret "$9$n8HX6A01RhLvL1R"; # SECRET-DATA
      }
    }
  }
  profile u {
    authentication-order radius;
  }
  radius-server {
    192.168.65.63 {
      port 1812;
      secret "$9$Vyb4ZHkPQ39mf9pORlexNdbgoZUjqP5"; # SECRET-DATA
    }
  }
}
services {
  l2tp {
    tunnel-group 1 {
      l2tp-access-profile t;
      ppp-access-profile u;
      local-gateway {
        address 10.70.1.1;
      }
      service-interface sp-1/3/0;
    }
    traceoptions {
      flag all;
      debug-level packet-dump;
      filter {
        protocol l2tp;
        protocol ppp;
        protocol radius;
      }
    }
  }
}
```

**Related  
Documentation**

- [L2TP Services Configuration Overview on page 579](#)
- [L2TP Minimum Configuration on page 580](#)
- [Configuring L2TP Tunnel Groups on page 582](#)
- [Tracing L2TP Operations on page 591](#)
- [Examples: Configuring L2TP Services on page 593](#)

## AS PIC Redundancy for L2TP Services

L2TP services support AS PIC redundancy. To configure redundancy, you specify a redundancy services PIC (**rsp**) interface in which the primary AS PIC is active and a secondary AS PIC is on standby. If the primary AS PIC fails, the secondary PIC becomes active, and all service processing is transferred to it. If the primary AS PIC is restored, it remains in standby and does not preempt the secondary AS PIC; you need to manually restore the services to the primary PIC. To determine which PIC is currently active, issue the **show interfaces redundancy** command.



**NOTE:** On L2TP, the only service option supported is *warm standby*, in which one backup PIC supports multiple working PICs. Recovery times are not guaranteed, because the configuration must be completely restored on the backup PIC after a failure is detected. The tunnels and sessions are torn down upon switchover and need to be restarted by the LAC and PPP client, respectively. However, configuration is preserved and available on the new active PIC, although the protocol state needs to be reestablished.

As with the other AS PIC services that support warm standby, you can issue the **request interfaces (revert | switchover)** command to manually switch between primary and secondary L2TP interfaces.

For more information, see “[Configuring AS or Multiservices PIC Redundancy](#)” on page 806. For an example configuration, see “[Examples: Configuring L2TP Services](#)” on page 593. For information on operational mode commands, see the [CLI Explorer](#).

### Related Documentation

- [Layer 2 Tunneling Protocol Overview](#) on page 78
- [L2TP Services Configuration Overview](#) on page 579
- [Configuring AS or Multiservices PIC Redundancy](#) on page 806
- [L2TP Minimum Configuration](#) on page 580
- [Examples: Configuring L2TP Services](#) on page 593

## IP Packet Fragment Reassembly for L2TP Overview

You can configure the service interfaces on the MX Series routers with modular port concentrators (MPCs) to support reassemble fragmented IP packets for an L2TP connection. When packets are transmitted over an L2TP connection, the packets may be fragmented during transmission and need to be reassembled before they are processed further. Efficient reassembly is important for network throughput, scalability, and graceful response to congestion.

Fragmentation of IP packets for transmission and the need to reassemble the IP packets at a destination is a feature of how Layer 2 (the frame layer) and Layer 3 (the packet layer) operate. The maximum size of a frame, set by the Maximum Transmission Unit (MTU) value, and the maximum size of a packet are determined independently. Typically

the packet size can far exceed the MTU size defined for the outgoing connection. If the packet size (data plus IP and other headers) exceeds the configured frame size (usually set by the transport medium limits), the packet must be fragmented and split across multiple frames for transmission. Frames are always processed immediately, when they arrive (if error-free), but packet fragments cannot be processed until the whole packet has been reassembled. Each packet fragment inside a frame series, except the last packet fragment, has the more fragments (MF) IP header bit set, indicating that this packet is part of a whole. The last packet fragment inside a frame does not have this MF bit set and therefore ends the fragment sequence. After all of the fragments of a packet have arrived, the entire packet can be reassembled.

In an L2TP connection, packets are transmitted between the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS). For an IP packet being transmitted over an L2TP connection, the packet is fragmented at the LAC, at an LNS, or at any intermediate router. IP reassembly parameters configured on the service interfaces of the LAC and the LNS determine how the fragments are reassembled at the service interfaces to ensure efficient reassembly over an L2TP connection.

**Related  
Documentation**

- [Configuring IP Inline Reassembly for L2TP on page 590](#)
- *Protocols and Applications Supported by MX240, MX480, MX960, MX2010, and MX2020 Enhanced MPCs (MPCEs)*
- *ip-reassembly*

---

## Configuring IP Inline Reassembly for L2TP

---

This procedure shows how to configure a service interface on a LAC or LNS to reassemble fragmented IP packets. This example creates a service set that configures the IP reassembly parameters for L2TP fragments. The service set is then associated with the L2TP service.

Before you configure inline IP reassembly, be sure you have:

- Configured L2TP.
- Configured a valid service interface on the LAC or LNS.

To configure inline IP reassembly:

1. Configure the chassis-level bandwidth used by the inline services interface on the FPC and PIC slot for inline IP fragment reassembly.

```
[edit chassis]
user@host# set fpc 2 pic 1 inline-services bandwidth 10g
```

2. Configure the interface-level logical unit used by the inline services (si-) interface on the FPC and PIC slot for inline IP fragment reassembly.

```
[edit interfaces]
user@host# set si-2/1/0 unit 0 family inet
user@host# set si-2/1/0 unit 0 service-domain inside
```



**NOTE:** This configuration is not unique to L2TP. However, you must configure the family (inet) and service domain (inside) as shown.

3. Configure the service set (**set1**) for IP reassembly in the input match direction. (The **local** option loops the reassembled packets back to the local interface.)

```
[edit services]
```

```
user@host# set service-set set1
```

```
[edit services service-set ip-reassembly-set]
```

```
user@host# set ip-reassembly-rules ipr_rule1
```

```
user@host# set next-hop-service inside-service-interface si-9/1/0.0
```

```
user@host# set next-hop-service outside-service-interface-type local
```



**NOTE:** You must configure both inside (si- interface) and outside type (**local**) service interfaces statements. The reassembly rule is not formulated outside of the service set; this statement simply initiates the reassembly process.

4. Configure the IP reassembly rule parameter

```
[edit services ip-reassembly]
```

```
user@host# set rule ipr_rule1 match-direction input;
```

5. Configure the service set (**set1**) for IP reassembly to bind to the L2TP service.



**NOTE:**

- The service set must be defined at the [edit services] hierarchy level.
- You cannot delete a service set instance if it is associated with an L2TP service.

```
[edit services l2tp]
```

```
user@host# set ip-reassembly service-set set1
```

#### Related Documentation

- [IP Packet Fragment Reassembly for L2TP Overview on page 589](#)
- [Configuring an L2TP LNS with Inline Service Interfaces](#)
- [Protocols and Applications Supported by MX240, MX480, MX960, MX2010, and MX2020 Enhanced MPCs \(MPCEs\)](#)

## Tracing L2TP Operations

Tracing operations track all AS PIC operations and record them in a log file in the `/var/log` directory. By default, this file is named `/var/log/l2tpd`.



**NOTE:** This topic refers to tracing L2TP LNS operations on M Series routers. To trace L2TP LAC operations on MX Series routers, see *Tracing L2TP Operations for Subscriber Access*.

To trace L2TP operations, include the **traceoptions** statement at the **[edit services l2tp]** hierarchy level:

```
traceoptions {  
  debug-level level;  
  file <filename> <files number> <match regular-expression > <size maximum-file-size>  
    <world-readable | no-world-readable>;  
  filter {  
    protocol name;  
    user-name username;  
  }  
  flag flag;  
  interfaces interface-name {  
    debug-level severity;  
    flag flag;  
  }  
  level (all | error | info | notice | verbose | warning);  
  no-remote-trace;  
}
```

You can specify the following L2TP tracing flags:

- **all**—Trace everything.
- **configuration**—Trace configuration events.
- **protocol**—Trace routing protocol events.
- **routing-socket**—Trace routing socket events.
- **rpd**—Trace routing protocol process events.

You can specify a trace level for PPP, L2TP, RADIUS, and User Datagram Protocol (UDP) tracing. To configure a trace level, include the **debug-level** statement at the **[edit services l2tp traceoptions]** hierarchy level and specify one of the following values:

- **detail**—Detailed debug information
- **error**—Errors only
- **packet-dump**—Packet decoding information

You can filter by protocol. To configure filters, include the **filter protocol** statement at the **[edit services l2tp traceoptions]** hierarchy level and specify one or more of the following protocol values:

- **ppp**
- **l2tp**

- **radius**
- **udp**

To implement filtering by protocol name, you must also configure either **flag protocol** or **flag all**.

You can also configure traceoptions for L2TP on a specific adaptive services interface. To configure per-interface tracing, include the **interfaces** statement at the **[edit services l2tp traceoptions]** hierarchy level:

```
interfaces interface-name {
  debug-level level;
  flag flag;
}
```



**NOTE:** Implementing traceoptions consumes CPU resources and affects the packet processing performance.

You can specify the **debug-level** and **flag** statements for the interface, but the options are slightly different from the general L2TP traceoptions. You specify the debug level as **detail**, **error**, or **extensive**, which provides complete PIC debug information. The following flags are available:

- **all**—Trace everything.
- **ipc**—Trace L2TP Inter-Process Communication (IPC) messages between the PIC and the Routing Engine.
- **packet-dump**—Dump each packet's content based on debug level.
- **protocol**—Trace L2TP, PPP, and multilink handling.
- **system**—Trace packet processing on the PIC.

#### Related Documentation

- [L2TP Services Configuration Overview on page 579](#)
- [L2TP Minimum Configuration on page 580](#)
- [Configuring L2TP Tunnel Groups on page 582](#)
- [Configuring the Identifier for Logical Interfaces that Provide L2TP Services on page 587](#)
- [Examples: Configuring L2TP Services on page 593](#)

## Examples: Configuring L2TP Services

Configure L2TP with multiple group and user profiles and a pool of logical interfaces for concurrent tunnel sessions:

```
[edit access]
address-pool customer_a {
  address 10.1.1.1/32;
}
```

```
address-pool customer_b {
  address-range low 10.2.2.1 high 10.2.3.2;
}
group-profile sunnyvale_users {
  ppp {
    framed-pool customer_a;
    idle-timeout 15;
    primary-dns 192.168.65.1;
    secondary-dns 192.168.65.2;
    primary-wins 192.168.65.3;
    secondary-wins 192.168.65.4;
    interface-id west;
  }
}
group-profile eastcoast_users {
  ppp {
    framed-pool customer_b;
    idle-timeout 20;
    primary-dns 192.168.65.5;
    secondary-dns 192.168.65.6;
    primary-wins 192.168.65.7;
    secondary-wins 192.168.65.8;
    interface-id east;
  }
}
group-profile sunnyvale_tunnel {
  l2tp {
    maximum-sessions-per-tunnel 100;
    interface-id west_shared;
  }
}
group-profile east_tunnel {
  l2tp {
    maximum-sessions-per-tunnel 125;
    interface-id east_shared;
  }
}
profile sunnyvale_bldg_1 {
  client white {
    chap-secret "$9$3s2690leK8X7VKM7VwgaJn/Ctu1hclv87Ct87"; # SECRET-DATA
    ppp {
      idle-timeout 22;
      primary-dns 192.168.65.1;
      framed-ip-address 10.12.12.12/32;
      interface-id east;
    }
    group-profile sunnyvale_users;
  }
  client blue {
    chap-secret "$9$eq1KWxbwgZUHNdjmqmTF3uO1Rhr-dsoJDNd"; # SECRET-DATA
    group-profile sunnyvale_users;
  }
  authentication-order password;
}
profile sunnyvale_bldg_1_tunnel {
  client test {
```

```

l2tp {
    shared-secret "$9$r3HKvLg4ZUDkX7JGjif5p0BIRS8LN"; # SECRET-DATA
    maximum-sessions-per-tunnel 75;
    interface-id west_shared;
    ppp-authentication chap;
}
group-profile sunnyvale_tunnel;
}
client production {
    l2tp {
        shared-secret
            "$9$R2QErV8X-goGylVwg4jiTz36/t0BEleWFnRhrlXxbs2aJDHqf3nCP5";
        ppp-authentication chap;
    }
    group-profile sunnyvale_tunnel;
}
}
[edit services]
l2tp {
    tunnel-group finance-lns-server {
        l2tp-access-profile sunnyvale_bldg_1_tunnel;
        ppp-access-profile sunnyvale_bldg_1;
        local-gateway {
            address 10.1.117.3;
        }
        service-interface sp-1/3/0;
        receive-window 1500;
        maximum-send-window 1200;
        retransmit-interval 5;
        hello-interval 15;
        tunnel-timeout 55;
    }
    traceoptions {
        flag all;
    }
}
[edit interfaces sp-1/3/0]
unit 0 {
    family inet;
}
unit 10 {
    dial-options {
        l2tp-interface-id foo-user;
        dedicated;
    }
    family inet;
}
unit 11 {
    dial-options {
        l2tp-interface-id east;
        dedicated;
    }
    family inet;
}
unit 12 {
    dial-options {

```

```
        l2tp-interface-id east;
        dedicated;
    }
    family inet;
}
unit 21 {
    dial-options {
        l2tp-interface-id west;
        dedicated;
    }
    family inet;
}
unit 30 {
    dial-options {
        l2tp-interface-id west_shared;
        shared;
    }
    family inet;
}
unit 40 {
    dial-options {
        l2tp-interface-id east_shared;
        shared;
    }
    family inet;
}
```

Configure L2TP redundancy:

```
interfaces {
    rsp0 {
        redundancy-options {
            primary sp-0/0/0;
            secondary sp-1/3/0;
        }
        unit 0 {
            family inet;
        }
        unit 11 {
            dial-options {
                l2tp-interface-id east_shared;
                shared;
            }
            family inet;
        }
    }
}
```

**Related  
Documentation**

- [L2TP Services Configuration Overview on page 579](#)
- [L2TP Minimum Configuration on page 580](#)
- [Configuring L2TP Tunnel Groups on page 582](#)
- [Configuring the Identifier for Logical Interfaces that Provide L2TP Services on page 587](#)
- [Tracing L2TP Operations on page 591](#)

## CHAPTER 22

# Summary of Layer 2 Tunneling Protocol Configuration Statements

The following sections explain each of the Layer 2 Tunneling Protocol (L2TP) statements. The statements are organized alphabetically.


### facility-override

---


<b>Syntax</b>	<code>facility-override <i>facility-name</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>group-name</i> <b>syslog host</b> <i>hostname</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Override the default facility for system log reporting.
<b>Options</b>	<b><i>facility-name</i></b> —Name of the facility that overrides the default assignment. Valid entries include:  <b>authorization</b>  <b>daemon</b>  <b>ftp</b>  <b>kernel</b>  <b>local0</b> through <b>local7</b>  <b>user</b>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Logging of L2TP Tunnel Activity on page 585</a></li></ul>

## hello-interval

---

<b>Syntax</b>	hello-interval <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the keepalive timer for L2TP tunnels.
<hr/>	
<div> <b>NOTE:</b> Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.</div> <hr/>	
<b>Options</b>	<b>seconds</b> —Interval, in seconds, after which the server sends a hello message if no messages are received. A value of <b>0</b> means that no hello messages are sent. <b>Default:</b> 60 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Timers for L2TP Tunnels on page 584</a></li><li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces</a></li></ul>

## hide-avps

<b>Syntax</b>	hide-avps;
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Hide L2TP attribute-value pairs if the secret shared between the two ends of the tunnel is known.
<div>  <b>NOTE:</b> This statement is not supported for L2TP LNS on MX Series routers. </div>	
<b>Default</b>	Attribute-value pairs that can be hidden are exposed, even if the secret information is known.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Hiding Attribute-Value Pairs for L2TP Tunnels on page 585</a></li> </ul>

## host (L2TP)

<b>Syntax</b>	<pre>host <i>hostname</i> {     <b>services</b> <i>severity-level</i>;     <b>facility-override</b> <i>facility-name</i>;     <b>log-prefix</b> <i>prefix-value</i>; }</pre>
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>group-name</i> <b>syslog</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the hostname for the system logging utility.
<b>Options</b>	<p><b>hostname</b>—Name of the system logging utility host machine. This can be the local Routing Engine or an external server address.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring System Logging of L2TP Tunnel Activity on page 585</a></li> </ul>

## ip-reassembly (L2TP)

---

<b>Syntax</b>	<code>ip-reassembly {     service-set <i>service-set-name</i>; }</code>
<b>Hierarchy Level</b>	[edit services l2tp]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.1.
<b>Description</b>	Associate the reassembly service-set with the L2TP service.



**NOTE:** The service set must be defined at the [edit services] hierarchy level.

---

<b>Options</b>	<b>service-set <i>service-set-name</i></b> —Identifies the service set to be associated with the L2TP service.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">IP Packet Fragment Reassembly for L2TP Overview on page 589</a></li><li>• <a href="#">Configuring IP Inline Reassembly for L2TP on page 590</a></li></ul>

## l2tp-access-profile

---

<b>Syntax</b>	<code>l2tp-access-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the profile used to validate all L2TP connection requests to the local gateway address.
<b>Options</b>	<b><i>profile-name</i></b> —Identifier for the L2TP connection profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Access Profiles for L2TP Tunnel Groups on page 583</a></li><li>• <a href="#">Configuring an L2TP Access Profile on the LNS</a></li></ul>

## local-gateway (L2TP LNS)

<b>Syntax</b>	local-gateway { address <i>address</i> ; gateway-name <i>gateway-name</i> ; }
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the IP address or name for the local (LNS) gateway for L2TP tunnel.  The remaining statements are explained separately.
<b>Options</b>	<b>address</b> —Local IP address; corresponds to the IP address that is used by LACs to identify the LNS. When the LAC is an MX Series router, this address matches the remote gateway address configured in the LAC tunnel profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Local Gateway Address and PIC on page 583.</a></li> <li>• <a href="#">Configuring L2TP Tunnel Groups on page 582</a></li> <li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces</a></li> </ul>

## log-prefix (L2TP)

<b>Syntax</b>	log-prefix <i>prefix-value</i> ;
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>group-name</i> <b>syslog host</b> <i>hostname</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Set the system logging prefix value.
<b>Options</b>	<b>prefix-value</b> —System logging prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring System Logging of L2TP Tunnel Activity on page 585</a></li> </ul>

## maximum-send-window

---

<b>Syntax</b>	<code>maximum-send-window <i>packets</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <a href="#">tunnel-group <i>name</i></a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the size of the send window for L2TP tunnels, which limits the remote end's receive window size.



**NOTE:** This statement is not supported for L2TP LNS on MX Series routers.

---

<b>Options</b>	<b><i>packets</i></b> —Maximum number of packets the send window can hold at one time. <b>Default:</b> 32
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Window Size for L2TP Tunnels on page 584</a></li></ul>

## ppp-access-profile

---

<b>Syntax</b>	<code>ppp-access-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <a href="#">tunnel-group <i>name</i></a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the profile used to validate all Point-to-Point Protocol (PPP) session requests through L2TP tunnels established to the local gateway address.



**NOTE:** This statement is not supported for L2TP LNS on MX Series routers.

---

<b>Options</b>	<b><i>profile-name</i></b> —Identifier for the PPP profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Access Profiles for L2TP Tunnel Groups on page 583</a></li></ul>

## receive-window

<b>Syntax</b>	<code>receive-window <i>packets</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services l2tp <b>tunnel-group</b> <i>name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the size of the receive window for L2TP tunnels, which limits the number of packets the server processes concurrently.



**NOTE:** This statement is not supported for L2TP LNS on MX Series routers.

<b>Options</b>	<b><i>packets</i></b> —Maximum number of packets the receive window can hold at one time. <b>Default:</b> 16
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Window Size for L2TP Tunnels on page 584</a></li> </ul>

## retransmit-interval (Services)

<b>Syntax</b>	<code>retransmit-interval <i>seconds</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services l2tp <b>tunnel-group</b> <i>name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the maximum retransmit interval for L2TP tunnels.




**NOTE:** This statement is not supported for L2TP LNS on MX Series routers.

<b>Options</b>	<b><i>seconds</i></b> —Interval, in seconds, after which the server retransmits data if no acknowledgment is received. <b>Default:</b> 30 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Timers for L2TP Tunnels on page 584</a></li> </ul>

## service-interface

---

<b>Syntax</b>	<code>service-interface <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Option <b>si-fpc/pic/port</b> introduced in Junos OS Release 11.4.
<b>Description</b>	Specify the service interface responsible for handling L2TP processing.
<div> <b>NOTE:</b> On MX Series routers, the service interface configuration is required for static LNS sessions. Either the service interface configuration or the service device pool configuration can be used for dynamic LNS sessions.</div>	
<b>Options</b>	<b><i>interface-name</i></b> —Name of the service interface. The interface type depends on the line card as follows: <ul style="list-style-type: none"><li>• <b>sp-fpc/pic/port</b>—On AS or Multiservices PICs on M7i, M10i, and M120 routers.</li><li>• <b>si-fpc/pic/port</b>—On MPCs on MX Series routers.</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Local Gateway Address and PIC on page 583</a></li><li>• <a href="#">Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces</a></li></ul>

## services

---

See the following sections:

- [services \(Hierarchy\) on page 605](#)
- [services \(L2TP System Logging\) on page 606](#)

### services (Hierarchy)

<b>Syntax</b>	<code>services l2tp { ... }</code>
<b>Hierarchy Level</b>	<a href="#">[edit]</a>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the service properties to be applied to traffic.
<b>Options</b>	<code>l2tp</code> —Identifies the L2TP set of services statements.
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">L2TP Services Configuration Overview on page 579</a></li></ul>

## services (L2TP System Logging)

<b>Syntax</b>	<code>services severity-level;</code>
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>group-name</i> <b>syslog host</b> <i>hostname</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the system logging severity level.
<b>Options</b>	<p><b>severity-level</b>—Assigns a severity level to the facility. Valid entries include:</p> <ul style="list-style-type: none"><li>• <b>alert</b>—Conditions that should be corrected immediately.</li><li>• <b>any</b>—Matches any level.</li><li>• <b>critical</b>—Critical conditions.</li><li>• <b>emergency</b>—Panic conditions.</li><li>• <b>error</b>—Error conditions.</li><li>• <b>info</b>—Informational messages.</li><li>• <b>notice</b>—Conditions that require special handling.</li><li>• <b>warning</b>—Warning messages.</li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Logging of L2TP Tunnel Activity on page 585</a></li></ul>

## syslog

**Syntax**    `syslog {  
                   host hostname {  
                     services severity-level;  
                     facility-override facility-name;  
                     log-prefix prefix-value;  
                   }  
                 }`

**Hierarchy Level**    [edit services l2tp **tunnel-group** *group-name*]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure the generation of system log messages for L2TP services. System log information is passed to the kernel for logging in the `/var/log/l2tpd` directory.



**NOTE:** This statement is not supported for L2TP LNS on MX Series routers.

**Options**    The remaining statements are described separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                       interface-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring System Logging of L2TP Tunnel Activity on page 585](#)

## traceoptions (L2TP)

---

**Syntax**    `traceoptions {  
          debug-level level;  
          file filename <files number> <match regular-expression > <size maximum-file-size>  
                  <world-readable | no-world-readable>;  
          filter {  
            protocol name;  
            user user@domain;  
            user-name username;  
          }  
          flag flag;  
          interfaces interface-name {  
            debug-level level;  
            flag flag;  
          }  
          level (all | error | info | notice | verbose | warning);  
          no-remote-trace;  
          }`

**Hierarchy Level**    [edit services l2tp]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Define tracing operations for L2TP processes.

**Options**    **debug-level *level***—Trace level for PPP, L2TP, RADIUS, and UDP; this option does not apply to L2TP on MX Series routers:

- **detail**—Trace detailed debug information.
- **error**—Trace error information.
- **packet-dump**—Trace packet decoding information.

**file *filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`.

**files *number***—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

**Range:** 2 through 1000

**Default:** 3 files

**filter**—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifiers simplifies troubleshooting in a scaled environment.

- **protocol *name***—One of the following protocols; this option does not apply to L2TP on MX Series routers:
  - **l2tp**

- **ppp**
- **radius**
- **udp**
- **user** *user@domain*—Username of a subscriber; this option does not apply to L2TP on M Series routers. Optionally use an asterisk (\*) as a wildcard to substitute for characters at the beginning or end of either term or both terms.
- **user-name** *username*—Username of a subscriber; this option does not apply to L2TP on MX Series routers.

**flag** *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **configuration**—Trace configuration events.
- **events**—Trace interface events.
- **general**—Trace general events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization.
- **ipc-rx**—Trace IPC receive events.
- **ipc-tx**—Trace IPC transmit events.
- **memory**—Trace memory management code.
- **message**—Trace message processing code.
- **packet-error**—Trace packet error events.
- **parse**—Trace parsing events.
- **protocol**—Trace L2TP events.
- **receive-packets**—Trace received L2TP packets.
- **routing-process**—Trace routing process interactions.
- **routing-socket**—Trace routing socket events.
- **session-db**—Trace session database interactions.
- **states**—Trace state machine events.
- **timer**—Trace timer events.
- **transmit-packets**—Trace transmitted L2TP packets.
- **tunnel**—Trace tunnel events.

**interfaces *interface-name***—Apply L2TP traceoptions to a specific services interface. This option does not apply to L2TP on MX Series routers.

- **debug-level *level***—Trace level for the interface; this option does not apply to L2TP on MX Series routers:
  - **detail**—Trace detailed debug information.
  - **error**—Trace error information.
  - **extensive**—Trace all PIC debug information.
- **flag *flag***—Tracing operation to perform for the interface. This option does not apply to L2TP on MX Series routers. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:
  - **all**—Trace everything.
  - **ipc**—Trace L2TP Inter-Process Communication (IPC) messages between the PIC and the Routing Engine.
  - **packet-dump**—Dump each packet content based on debug level.
  - **protocol**—Trace L2TP, PPP, and multilink handling.
  - **system**—Trace packet processing on the PIC.

**level**—Specify level of tracing to perform. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

**Default:** error

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size maximum-file-size**—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** **sizek** to specify KB, **sizem** to specify MB, or **sizeg** to specify GB

**Range:** 10240 through 1073741824

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege Level</b>	trace—To view this statement in the configuration.
	trace-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Tracing L2TP Operations on page 591</a></li></ul>
	<ul style="list-style-type: none"><li>• <i>Tracing L2TP Operations for Subscriber Access</i></li></ul>

## tunnel-group

**Syntax** `tunnel-group group-name {  
     aaa-access-profile profile-name;  
     dynamic-profile profile-name;  
     hello-interval seconds;  
     hide-avps;  
     l2tp-access-profile profile-name;  
     local-gateway address {  
         address address;  
         gateway-name gateway-name;  
     }  
     maximum-send-window packets;  
     ppp-access-profile profile-name;  
     receive-window packets;  
     retransmit-interval seconds;  
     service-device-pool pool-name;  
     service-interface interface-name;  
     syslog {  
         host hostname {  
             services severity-level;  
             facility-override facility-name;  
             log-prefix prefix-value;  
         }  
     }  
     tos-reflect;  
     tunnel-switch-profile profile-name;  
     tunnel-timeout seconds;  
 }`

**Hierarchy Level** [edit services l2tp]

**Release Information** Statement introduced before Junos OS Release 7.4.  
 Support for MX Series routers introduced in Junos OS Release 11.4.

**Description** Specify the L2TP tunnel properties.



**NOTE:** Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

**Options** *group-name*—Identifier for the tunnel group.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
 interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring L2TP Tunnel Groups on page 582](#)
- [Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces](#)

## tunnel-timeout

---

<b>Syntax</b>	tunnel-timeout <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit services l2tp <b>tunnel-group</b> <i>name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the maximum downtime for an L2TP tunnel, after which the tunnel is terminated because the connection is presumed to have been lost.
<b>Options</b>	<b>seconds</b> —Interval after which the tunnel is terminated if no data can be sent. <b>Default:</b> 120 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Timers for L2TP Tunnels on page 584</a></li><li>• <i>Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces</i></li></ul>



# Link Services IQ Interfaces Configuration Guidelines

You can configure link services intelligent queuing (IQ) (LSQ or **lsq-**) interfaces on the Adaptive Services (AS) PIC, the internal Adaptive Services Module in the M7i platform, the Link Services II PIC, and the Multiservices PIC. LSQ interfaces are similar to link services interfaces, which are described in [“Multilink and Link Services Logical Interface Configuration Overview” on page 1385](#). The important difference is that LSQ interfaces fully support Junos class of service (CoS) components.

The AS or Multiservices PIC has a limit of 1023 logical interfaces. Each logical interface is a Multilink Point-to-Point Protocol (MLPPP) bundle, an FRF.15 bundle, or an FRF.16 DLCI.

This chapter describes the Layer 2 service package and the CoS and failure recovery capabilities of LSQ interfaces. For detailed information about Layer 3 services, see other chapters in this manual and the *Junos OS, Release 14.1*.



**NOTE:** The Link Services II PIC offers the same functionality as the Layer 2 service package on AS or Multiservices PICs.

This chapter contains the following sections:

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS on page 618](#)
- [Configuring LSQ Interface Redundancy in a Single Router Using SONET APS on page 620](#)
- [Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621](#)
- [Configuring CoS Scheduling Queues on Logical LSQ Interfaces on page 630](#)
- [Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces on page 633](#)
- [Reserving Bundle Bandwidth for Link-Layer Overhead on LSQ Interfaces on page 635](#)
- [Configuring Multiclass MLPPP on LSQ Interfaces on page 636](#)
- [Oversubscribing Interface Bandwidth on LSQ Interfaces on page 638](#)

- [Configuring Guaranteed Minimum Rate on LSQ Interfaces on page 643](#)
- [Configuring Link Services and CoS on Services PICs on page 646](#)
- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using MLPPP on page 649](#)
- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using FRF.16 on page 655](#)
- [Configuring LSQ Interfaces for Single Fractional T1 or El Interfaces Using MLPPP and LFI on page 660](#)
- [Configuring LSQ Interfaces for Single Fractional T1 or El Interfaces Using FRF.12 on page 665](#)
- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using FRF.15 on page 672](#)
- [Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP on page 673](#)
- [Configuring LSQ Interfaces as T3 or OC3 Bundles Using FRF.12 on page 675](#)
- [Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP on page 677](#)

---

## Layer 2 Service Package Capabilities and Interfaces

---

As described in [“Enabling Service Packages” on page 41](#), you can configure the AS or Multiservices PIC and the internal ASM in the M7i platform to use either the Layer 2 or the Layer 3 service package.

When you enable the Layer 2 service package, the AS or Multiservices PIC supports *link services*. On the AS or Multiservices PIC and the ASM, link services include the following:

- Junos CoS components—[“Configuring CoS Scheduling Queues on Logical LSQ Interfaces” on page 630](#) describes how the Junos CoS components work on link services IQ (**lsq**) interfaces. For detailed information about Junos CoS components, see the *Junos OS Class of Service Library for Routing Devices*.
- Data compression using the compressed Real-Time Transport Protocol (CRTP) for use in voice over IP (VoIP) transmission.



**NOTE:** On LSQ interfaces, all multilink traffic for a single bundle is sent to a single processor. If CRTP is enabled on the bundle, it adds overhead to the CPU. Because T3 network interfaces support only one link per bundle, make sure you configure a fragmentation map for compressed traffic on these interfaces and specify the no-fragmentation option. For more information, see [“Configuring Delay-Sensitive Packet Interleaving” on page 698](#) and [“Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces” on page 633](#).

- Link fragment interleaving (LFI) on Frame Relay links using FRF.12 end-to-end fragmentation—The standard for FRF.12 is defined in the specification FRF.12, *Frame Relay Fragmentation Implementation Agreement*.
- LFI on Multilink Point-to-Point Protocol (MLPPP) links.

- Multilink Frame Relay (MLFR) end-to-end (FRF.15)—The standard for FRF.15 is defined in the specification FRF.15, *End-to-End Multilink Frame Relay Implementation Agreement*.
- Multilink Frame Relay (MLFR) UNI NNI (FRF.16)—The standard for FRF.16 is defined in the specification FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*.
- MLPPP—The standard for MLPPP is defined in the specification RFC 1990, *The PPP Multilink Protocol (MP)*.
- Multiclass extension to MLPPP—The standard is defined in the specification RFC 2686, *The Multi-Class Extension to Multi-Link PPP*.

For the LSQ interface on the AS or Multiservices PIC, the configuration syntax is almost the same as for Multilink and Link Services PICs. The primary difference is the use of the interface-type descriptor **lsq** instead of **ml** or **ls**. When you enable the Layer 2 service package on the AS or Multiservices PIC, the following interfaces are automatically created:

```
gr-fpc/pic/port
ip-fpc/pic/port
lsq-fpc/pic/port
lsq-fpc/pic/port:0
...
lsq-fpc/pic/port:N
mt-fpc/pic/port
pd-fpc/pic/port
pe-fpc/pic/port
sp-fpc/pic/port
vt-fpc/pic/port
```

Interface types **gr**, **ip**, **mt**, **pd**, **pe**, and **vt** are standard tunnel interfaces that are available on the AS or Multiservices PIC whether you enable the Layer 2 or the Layer 3 service package. These tunnel interfaces function the same way for both service packages, except that the Layer 2 service package does not support some tunnel functions, as shown in Table 5 on page 24. For more information about tunnel interfaces, see *Tunnel Properties*.



**NOTE:** Interface type **sp** is created because it is needed by the Junos OS. For the Layer 2 service package, the **sp** interface is not configurable, but you should not disable it.

Interface type **lsq-fpc/pic/port** is the physical link services IQ interface (**lsq**). Interface types **lsq-fpc/pic/port:0** through **lsq-fpc/pic/port:N** represent FRF.16 bundles. These interface types are created when you include the **mlfr-uni-nni-bundles** statement at the **[edit chassis fpc slot-number pic pic-number]** hierarchy level. For more information, see “Configuring CoS Scheduling Queues on Logical LSQ Interfaces” on page 630.



**NOTE:** On DS0, E1, or T1 interfaces in LSQ bundles, you can configure the **bandwidth** statement, but the router does not use the bandwidth value if the interfaces are included in an MLPPP or MLFR bundle. The bandwidth is calculated internally according to the time slots, framing, and byte-encoding of the interface. For more information about these properties, see the *Junos OS Network Interfaces Library for Routing Devices*.

## Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS

Link services IQ (**lsq-**) interfaces that are paired with SONET PICs can use the Automatic Protection Switching (APS) configuration already available on SONET networks to provide failure recovery. SONET APS provides stateless failure recovery, if it is configured on SONET interfaces in separate chassis and each SONET PIC is paired with an AS or Multiservices PIC in the same chassis. If one of the following conditions for APS failure is met, the associated SONET PIC triggers recovery to the backup circuit and its associated AS or Multiservices PIC. The failure conditions are:

- Failure of Link Services IQ PIC
- Failure of FPC that hosts the Link Services IQ PIC
- Failure of Packet Forwarding Engine
- Failure of chassis

The guidelines for configuring SONET APS are described in the *Junos OS Network Interfaces Library for Routing Devices*.

The following sections describe how to configure failover properties:

- [Configuring the Association between LSQ and SONET Interfaces on page 618](#)
- [Configuring SONET APS Interoperability with Cisco Systems FRF.16 on page 619](#)
- [Restrictions on APS Redundancy for LSQ Interfaces on page 620](#)

### Configuring the Association between LSQ and SONET Interfaces

To configure the association between AS or Multiservices PICs hosting link services IQ interfaces and the SONET interfaces, include the **lsq-failure-options** statement at the **[edit interfaces]** hierarchy level:

```
lsq-fpc/pic/port {
  lsq-failure-options {
    no-termination-request;
    [ trigger-link-failure interface-name ];
  }
}
```

For example, consider the following network scenario:

- Primary router includes interfaces **oc3-0/2/0** and **lsq-1/1/0**.
- Backup router includes interfaces **oc3-2/2/0** and **lsq-3/2/0**.

Configure SONET APS, with **oc3-0/2/0** as the working circuit and **oc3-2/2/0** as the protect circuit. Include the **trigger-link-failure** statement to extend failure to the LSQ PICs:

```
interfaces lsq-1/1/0 {
  lsq-failure-options {
    trigger-link-failure oc3-0/2/0;
  }
}
```



**NOTE:** You must configure the **lsq-failure-options** statement on the primary router only. The configuration is not supported on the backup router.

To inhibit the router from sending PPP termination-request messages to the remote host if the Link Services IQ PIC fails, include the **no-termination-request** statement at the **[edit interfaces lsq-fpc/pic/port lsq-failure-options]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port lsq-failure-options]
no-termination-request;
```

This functionality is supported on link PICs as well. To inhibit the router from sending PPP termination-request messages to the remote host if a link PIC fails, include the **no-termination-request** statement at the **[edit interfaces interface-name ppp-options]** hierarchy level.

```
[edit interfaces interface-name ppp-options]
no-termination-request;
```

The **no-termination-request** statement is supported only with MLPPP and SONET APS configurations and works with PPP, PPP over Frame Relay, and MLPPP interfaces only, on the following PICs:

- Channelized OC3 IQ PICs
- Channelized OC12 IQ PICs
- Channelized STM1 IQ PICs
- Channelized STM4 IQ PICs

## Configuring SONET APS Interoperability with Cisco Systems FRF.16

Juniper Networks routers configured with APS might not interoperate correctly with Cisco FRF.16. To enable interoperation, include the **cisco-interoperability** statement at the **[edit interfaces lsq-fpc/pic/port mlfr-uni-nni-bundle-options]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port mlfr-uni-nni-bundle-options]
cisco-interoperability send-lip-remove-link-for-link-reject;
```

The **send-lip-remove-link-for-link-reject** option prompts the router to send a Link Integrity Protocol remove link when it receives an add-link rejection message.

## Restrictions on APS Redundancy for LSQ Interfaces

The following restrictions apply to LSQ failure recovery:

- It applies only to Link Services IQ PICs installed in M Series routers, except for M320 routers.
- You must configure the **failure-options** statement on physical LSQ interfaces, not on MLFR channelized units.
- The Link Services IQ PICs must be associated with SONET link PICs. The paired PICs can be installed on different routers or in the same router; in other words, both interchassis and intrachassis recovery are supported
- Failure recovery is stateless; as a result, route flapping and loss of link state is expected in interchassis recovery, requiring PPP renegotiation. In intrachassis recovery, no impact on traffic is anticipated with Routing Engine failover, but PIC failover results in PPP renegotiation.
- The switchover is not revertive: when the original hardware is restored to service, traffic does not automatically revert back to it.
- Normal APS switchover and PIC-triggered APS switchover can be distinguished only by checking the system log messages.



**NOTE:** When an AS PIC experiences persistent back pressure as a result of high traffic volume for 3 seconds, the condition triggers an automatic core dump and reboot of the PIC to help clear the blockage. A system log message at level LOG\_ERR is generated. This mechanism applies to both Layer 2 and Layer 3 service packages.

---

### Related Documentation

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interface Redundancy in a Single Router Using SONET APS on page 620](#)
- [Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621](#)
- [Configuring Link Services and CoS on Services PICs on page 646](#)
- [Link Services Configuration for Junos Interfaces](#)

---

## Configuring LSQ Interface Redundancy in a Single Router Using SONET APS

Stateless switchover from one Link Services IQ PIC to another within the same router can be configured by using the SONET APS mechanism described in “[Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS](#)” on page 618. Each Link Services IQ PIC must be associated with a specified SONET link PIC within the same router.



**NOTE:** For complete intrachassis recovery, including recovery from Routing Engine failover, graceful Routing Engine switchover (GRES) must be enabled on the router. For more information, see the *Junos OS Administration Library for Routing Devices*.

#### Related Documentation

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621](#)
- [Configuring Link Services and CoS on Services PICs on page 646](#)
- [Link Services Configuration for Junos Interfaces](#)

## Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces

You can configure failure recovery on M Series, MX Series, and T Series routers that have multiple AS or Multiservices PICs and DPCs with **lsq**- interfaces by specifying a virtual LSQ redundancy (**rlsq**) interface in which the primary Link Services IQ PIC is active and a secondary PIC is on standby. If the primary PIC fails, the secondary PIC becomes active, and all LSQ processing is transferred to it. To determine which PIC is currently active, issue the **show interfaces redundancy** command.



**NOTE:** This configuration does not require the use of SONET APS for failover. Network interfaces that do not support SONET can be used, such as T1 or E1 interfaces.

The following sections provide more information:

- [Configuring Redundant Paired LSQ Interfaces on page 621](#)
- [Restrictions on Redundant LSQ Interfaces on page 622](#)
- [Configuring Link State Replication for Redundant Link PICs on page 624](#)
- [Examples: Configuring Redundant LSQ Interfaces for Failure Recovery on page 625](#)

## Configuring Redundant Paired LSQ Interfaces

The physical interface type **rlsq** specifies the pairings between primary and secondary **lsq** interfaces to enable redundancy. To configure a backup **lsq** interface, include the **redundancy-options** statement at the **[edit interfaces rlsqnumber]** hierarchy level:

```
[edit interfaces rlsqnumber]
redundancy-options {
  (hot-standby | warm-standby);
  primary lsq-fpc/pic/port;
  secondary lsq-fpc/pic/port;
}
```

For the **rlsq** interface, **number** can be from 0 through 1023. If the primary **lsq** interface fails, traffic processing switches to the secondary interface. The secondary interface remains active even after the primary interface recovers. If the secondary interface fails and the primary interface is active, processing switches to the primary interface.

The **hot-standby** option is used with one-to-one redundancy configurations, in which one working PIC is supported by one backup PIC. It is supported with MLPPP, CRTP, FRF.15, and FRF.16 configurations for the LSQ interface to achieve an uninterrupted LSQ service. It sets the requirement for the failure detection and recovery time to be less than 5 seconds. The behavior is revertive, but you can manually switch between the primary and secondary PICs by issuing the **request interfaces (revert | switchover) rlsqnumber** operational mode command. It also provides a switch over time of 5 seconds and less for FRF.15 and a maximum of 10 seconds for FRF.16.

The **warm-standby** option is used with redundancy configurations in which one backup PIC supports multiple working PICs. Recovery times are not guaranteed, because the configuration must be completely restored on the backup PIC after a failure is detected.

Certain combinations of **hot-standby** and **warm-standby** configuration are not permitted and result in a configuration error. The following examples are permitted:

- Interface **rlsq0** configured with **primary lsq-0/0/0** and **warm-standby**, in combination with interface **rlsq0:0** configured with **primary lsq-0/0/0:0**
- Interface **rlsq0:0** configured with **primary lsq-0/0/0:0**, in combination with interface **rlsq0:1** configured with **primary lsq-0/0/0:1**

The following example combinations are not permitted:

- Interface **rlsq0** configured with **primary lsq-0/0/0** and **hot-standby**, in combination with interface **rlsq0:0** configured with **primary lsq-0/0/0:0**
- Interface **rlsq0:0** configured with **primary lsq-0/0/0:0**, in combination with interface **rlsq1:0** configured with **primary lsq-0/0/0:0**
- Interface **rlsq0:0** configured with **primary lsq-0/0/0:1**, in combination with interface **rlsq1:1** configured with **primary lsq-0/0/0:1**
- Interface **rlsq0** configured with **primary lsq-0/0/0**, in combination with interface **rlsq1** configured with **primary lsq-0/0/0**

In addition, the same physical interface cannot be reused as the primary interface for more than one **rlsq** interface, nor can any of the associated logical interfaces. For example, primary interface **lsq-0/0/0** cannot be reused in another **rlsq** interface as **lsq-0/0/0:0**.

## Restrictions on Redundant LSQ Interfaces

Link Services IQ PIC failure occurs under the following conditions:

- The primary PIC fails to boot. In this case, the **rlsq** interface does not come up and manual intervention is necessary to reboot or replace the PIC, or to rename the primary PIC to the secondary one in the **rlsq** configuration.
- When configuring an **rlsq** interface, ensure that:

- The unit number allocated to the **rlsq** interface is less than the number of Multilink Frame Relay user-to-network interface network-to-network interface (UNI-NNI) (FRF.16) bundles allocated on the Link Services PIC.
- Data-link connection identifier (DLCI) is configured for the **rlsq** interface.

If these conditions are not met, the **rlsq** interface does not boot. When you issue the **show interfaces redundancy** command, the state of the **rlsq** interface is indicated as **Waiting for primary MS PIC**.

- The primary PIC becomes active and then fails. The secondary PIC automatically takes over processing.
- A failover to the secondary PIC takes place. The secondary PIC then fails. If the primary PIC has been restored to active state, processing switches to it.
- The FPC that contains the Link Services IQ PIC fails.

The following constraints apply to redundant LSQ configurations:

- We recommend that primary and secondary PICs be configured in two different FPCs (in chassis other than M10i routers).
- You cannot configure a Link Services IQ PIC with explicit bundle configurations and as a constituent of an **rlsq** interface.
- Redundant LSQ configurations provide full GRES support. (You must configure GRES at the **[edit chassis]** hierarchy level; see the *Junos OS Administration Library for Routing Devices*.)
- If you configure the **redundancy-options** statement with the **hot-standby** option, the configuration must include one **primary** interface value and one **secondary** interface value.
- Since the same interface name is used for **hot-standby** and **warm-standby**, if you modify the configuration to change this attribute, it is recommended that you first deactivate the interface, commit the new configuration, and then reactivate the interface.
- You cannot make changes to an active **redundancy-options** configuration. You must deactivate the **rlsqnumber** interface configuration, change it, and reactivate it.
- The **rlsqnumber** configuration becomes active only if the primary interface is active. When the configuration is first activated, the primary interface must be active; if not, the **rlsq** interface waits until the primary interface comes up.
- You cannot modify the configuration of **lsq** interfaces after they have been included in an active **rlsq** interface.
- All the operational mode commands that apply to **rsp** interfaces also apply to **rlsq** interfaces. You can issue **show** commands for the **rlsq** interface or the primary and secondary **lsq** interfaces. However, statistics on the link interfaces are not carried over following a Routing Engine switchover.
- The **rlsq** interfaces also support the **lsq-failure-options** configuration, discussed in [“Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS” on page 618](#). If the primary and secondary Link Services IQ PICs fail and the

**lsq-failure-options** statement is configured, the configuration triggers a SONET APS switchover.

- Redundant LSQ configurations that require MLPPP Multilink Frame Relay (FRF.15 and FRF.16) are supported only with the **warm-standby** option.
- Redundant LSQ support is extended to ATM network interfaces.
- Channelized interfaces are used with FRF-16 bundles, for example **rlsq0:0**. The **rlsq** number and its constituents, the **primary** and **secondary** interfaces, must match for the configuration to be valid: either all must be channelized, or none. For an example of an FRF.16 configuration, see [“Configuring LSQ Interface Redundancy for an FRF.16 Bundle” on page 629](#).



**NOTE:** Adaptive Services and Multiservices PICs in layer-2 mode (running Layer 2 services) are not rebooted when a MAC flow-control situation is detected.

---

## Configuring Link State Replication for Redundant Link PICs

*Link state replication*, also called *interface preservation*, is an addition to the SONET Automatic Protection Switching (APS) functionality that helps promote redundancy of the link PICs used in LSQ configurations.

Link state replication provides the ability to add two sets of links, one from the active (working) SONET PIC and the other from the backup (protect) SONET PIC to the same bundle. If the active SONET PIC fails, links from the standby PIC are used without causing a link renegotiation. All the negotiated state is replicated from the active links to the standby links to prevent link renegotiation. For more information about SONET APS configurations, see the *Junos OS Network Interfaces Library for Routing Devices*.

To configure link state replication, include the **preserve-interface** statement at the **[edit interfaces interface-name sonet-options aps]** hierarchy level on both network interfaces:

```
edit interfaces interface-name sonet-options aps]
  preserve-interface;
```

The following constraints apply to link PIC redundancy:

- APS functionality must be available on the SONET PICs and the interface configurations must be identical on both ends of the link. Any configuration mismatch causes the commit operation to fail.
- This feature is supported only with LSQ and SONET APS-enabled link PICs, including Channelized OC3, Channelized OC12, and Channelized STM1 intelligent queuing (IQ) PICs.
- Link state replication supports MLPPP and PPP over Frame Relay (**frame-relay-ppp**) encapsulation, and fully supports GRES.
- Enabling the interface or protocol traceoptions with a large number of MLPPP links can trigger Link Control Protocol (LCP) renegotiation during the link switchover time.



**NOTE:** This renegotiation is more likely to take place for configurations with back-to-back Juniper Networks routers than in networks in which a Juniper Networks router is connected to an add/drop multiplexer (ADM).

- In general, networks that connect a Juniper Networks router to an ADM allow faster MLPPP link switchover than those with back-to-back Juniper Networks routers. The MLPPP link switchover time difference may be significant, especially for networks with a large number of MLPPP links.
- An aggressive LCP keepalive timeout configuration can lead to LCP renegotiation during the MLPPP link switchover. By default, the LCP keepalive timer interval is 10 seconds and the consecutive link down count is 3. The MLPPP links start LCP negotiation only after a timeout of 30 seconds. Lowering these configuration values may trigger one or more of the MLPPP links to renegotiate during the switchover time.



**NOTE:** LCP renegotiation is more likely to take place for configurations with back-to-back Juniper Networks routers than in networks in which a Juniper Networks router is connected to an ADM.

As an example, the following configuration shows the link state replication configuration between the ports `coc3-1/0/0` and `coc3-2/0/0`.

```
interfaces {
  coc3-1/0/0 {
    sonet-options {
      aps {
        preserve-interface;
        working-circuit aps-group-1;
      }
    }
  }
  coc3-2/0/0 {
    sonet-options {
      aps {
        preserve-interface;
        protect-circuit aps-group-1;
      }
    }
  }
}
```

## Examples: Configuring Redundant LSQ Interfaces for Failure Recovery

### Configuring LSQ Interface Redundancy for MLPPP

The following configuration shows that `lsq-1/1/0` and `lsq-1/3/0` work as a pair and the redundancy type is **hot-standby**, which sets the requirement for the failure detection and recovery time to be less than 5 seconds:

```

interfaces rlsq0 {
  redundancy-options {
    primary lsq-1/1/0;
    secondary lsq-1/3/0;
    hot-standby; #either hot-standby or warm-standby is supported
  }
}

```

The following example shows a related MLPPP configuration:



**NOTE:** MLPPP protocol configuration is required for this configuration.

```

interfaces {
  t1-/1/2/0 {
    unit 0 {
      family mlppp {
        bundle rlsq0.0;
      }
    }
  }
  rlsq0 {
    unit 0 {
      family inet {
        address 30.1.1.2/24;
      }
    }
  }
}

```

The following example shows a related CoS configuration:

```

class-of-service {
  interfaces {
    rlsq0 {
      unit * {
        fragmentation-maps fr-map1;
      }
    }
  }
}

```

The following example shows a complete link state replication configuration for MLPPP. This example uses two bundles, each with four T1 links. The first four T1 links (**t1-\*:1** through **t1-\*:4**) form the first bundle and the last four T1 links (**t1-\*:5** through **t1-\*:8**) form the second bundle. To minimize the duplication in the configuration, this example uses the **[edit groups]** statement; for more information, see the *Junos OS Administration Library for Routing Devices*. This type of configuration is not required; it simplifies the task and minimizes duplication.

```

groups {
  ml-partition-group {
    interfaces {
      <coc3-*> {
        partition 1 oc-slice 1 interface-type coc1;
      }
    }
  }
}

```

```

    }
    <coc1-*> {
        partition 1-8 interface-type t1;
    }
}
ml-bundle-group-1 {
    interfaces {
        <t1-*:"[1-4]"> {
            encapsulation ppp;
            unit 0 {
                family mlppp {
                    bundle lsq-0/1/0.0;
                }
            }
        }
    }
}
ml-bundle-group-2 {
    interfaces {
        <t1-*:"[5-8]"> {
            encapsulation ppp;
            unit 0 {
                family mlppp {
                    bundle lsq-0/1/0.1;
                }
            }
        }
    }
}
interfaces {
    lsq-0/1/0 {
        unit 0 {
            encapsulation multilink-ppp;
            family inet {
                address 1.1.1/32 {
                    destination 1.1.1.2;
                }
            }
        }
        unit 1 {
            encapsulation multilink-ppp;
            family inet {
                address 1.1.2/32 {
                    destination 1.1.2.2;
                }
            }
        }
    }
}
coc3-1/0/0 {
    apply-groups ml-partition-group;
    sonet-options {
        aps {
            preserve-interface;
            working-circuit aps-group-1;
        }
    }
}

```

```
    }  
  }  
}  
coc1-1/0/0:1 {  
  apply-groups ml-partition-group;  
}  
t1-1/0/0:1:1 {  
  apply-groups ml-bundle-group-1;  
}  
t1-1/0/0:1:2 {  
  apply-groups ml-bundle-group-1;  
}  
t1-1/0/0:1:3 {  
  apply-groups ml-bundle-group-1;  
}  
t1-1/0/0:1:4 {  
  apply-groups ml-bundle-group-1;  
}  
t1-1/0/0:1:5 {  
  apply-groups ml-bundle-group-2;  
}  
t1-1/0/0:1:6 {  
  apply-groups ml-bundle-group-2;  
}  
t1-1/0/0:1:7 {  
  apply-groups ml-bundle-group-2;  
}  
t1-1/0/0:1:8 {  
  apply-groups ml-bundle-group-2;  
}  
coc3-2/0/0 {  
  apply-groups ml-partition-group;  
  sonet-options {  
    aps {  
      preserve-interface;  
      protect-circuit aps-group-1;  
    }  
  }  
}  
coc1-2/0/0:1 {  
  apply-groups ml-partition-group;  
}  
t1-2/0/0:1:1 {  
  apply-groups ml-bundle-group-1;  
}  
t1-2/0/0:1:2 {  
  apply-groups ml-bundle-group-1;  
}  
t1-2/0/0:1:3 {  
  apply-groups ml-bundle-group-1;  
}  
t1-2/0/0:1:4 {  
  apply-groups ml-bundle-group-1;  
}  
t1-2/0/0:1:5 {  
  apply-groups ml-bundle-group-2;
```

```

}
t1-2/0/0:1:6 {
    apply-groups ml-bundle-group-2;
}
t1-2/0/0:1:7 {
    apply-groups ml-bundle-group-2;
}
t1-2/0/0:1:8 {
    apply-groups ml-bundle-group-2;
}
}

```

### Configuring LSQ Interface Redundancy for an FRF.15 Bundle

The following example shows a configuration for an FRF.15 bundle:

```

interfaces rlsq0 {
    redundancy-options {
        primary lsq-1/2/0;
        secondary lsq-1/3/0;
        warm-standby; #either hot-standby or warm-standby is supported
    }
    unit 0 {
        encapsulation multilink-frame-relay-end-to-end;
        family inet {
            address 30.1.1.1/24;
        }
    }
}

```

### Configuring LSQ Interface Redundancy for an FRF.16 Bundle

The following example shows a configuration for an FRF.16 bundle:

```

interfaces rlsq0:0 {
    dce;
    encapsulation multilink-frame-relay-uni-nni;
    redundancy-options {
        primary lsq-1/2/0:0;
        secondary lsq-1/3/0:0;
        warm-standby; #either hot-standby or warm-standby is supported
    }
    unit 0 {
        dlci 1000;
        family inet {
            address 50.1.1.1/24;
        }
    }
}

```

### Related Documentation

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS on page 618](#)

- [Configuring LSQ Interface Redundancy in a Single Router Using SONET APS on page 620](#)
- [Configuring Link Services and CoS on Services PICs on page 646](#)
- *Link Services Configuration for Junos Interfaces*

## Configuring CoS Scheduling Queues on Logical LSQ Interfaces

---

For link services IQ (**lsq-**) interfaces, you can specify a scheduler map for each logical unit. A logical unit represents either an MLPPP bundle or a DLCI configured on a FRF.16 bundle. The scheduler is applied to the traffic sent to an AS or Multiservices PIC running the Layer 2 link services package.

If you configure a scheduler map on a bundle, you must include the **per-unit-scheduler** statement at the **[edit interfaces lsq-fpc/pic/port]** hierarchy level. If you configure a scheduler map on an FRF.16 DLCI, you must include the **per-unit-scheduler** statement at the **[edit interfaces lsq-fpc/pic/port:channel]** hierarchy level. For more information, see the *Junos OS Class of Service Library for Routing Devices*.

If you need latency guarantees for multiclass or LFI traffic, you must use channelized IQ PICs for the constituent links. With non-IQ PICs, because queueing is not done at the channelized interface level on the constituent links, latency-sensitive traffic might not receive the type of service that it should. Constituent links from the following PICs support latency guarantees:

- Channelized E1 IQ PIC
- Channelized OC3 IQ PIC
- Channelized OC12 IQ PIC
- Channelized STM1 IQ PIC
- Channelized T3 IQ PIC

For scheduling queues on a logical interface, you can configure the following scheduler map properties at the **[edit class-of-service schedulers]** hierarchy level:

- **buffer-size**—The queue size; for more information, see [“Configuring Scheduler Buffer Size” on page 631](#).
- **priority**—The transmit priority (low, high, strict-high); for more information, see [“Configuring Scheduler Priority” on page 632](#).
- **shaping-rate**—The subscribed transmit rate; for more information, see [“Configuring Scheduler Shaping Rate” on page 632](#).
- **drop-profile-map**—The random early detection (RED) drop profile; for more information, see [“Configuring Drop Profiles” on page 632](#).

When you configure MLPPP and FRF.12 on M Series and T Series routers, you should configure a single scheduler with non-zero percent transmission rates and buffer sizes for queues 0 through 3, and assign this scheduler to the link services IQ interface (**lsq**) and to each constituent link.

When you configure FRF.16 on M Series and T Series routers, you can assign a single scheduler map to the link services IQ interface (**lsq**) and to each link services IQ DLCI, or you can assign different scheduler maps to the various DLCIs of the bundle, as shown in “[Example: Configuring an LSQ Interface as an NxT1 Bundle Using FRF.16](#)” on page 658. For the constituent links of an FRF.16 bundle, you do not need to configure a custom scheduler. Because LFI and multiclass are not supported for FRF.16, the traffic from each constituent link is transmitted from queue 0. This means you should allow most of the bandwidth to be used by queue 0. The default scheduler transmission rate and buffer size percentages for queues 0 through 3 are 95, 0, 0, and 5 percent, respectively. This default scheduler sends all user traffic to queue 0 and all network-control traffic to queue 3, and therefore it is well suited to the behavior of FRF.16. You can configure a custom scheduler that explicitly replicates the 95, 0, 0, and 5 percent queuing behaviors, and apply it to the constituent links.



**NOTE:** On T Series and M320 routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

For link services IQ interfaces (**lsq**), these scheduling properties work as they do in other PICs, except as noted in the following sections.



**NOTE:** On T Series and M320 routers, **lsq** interfaces do not support DiffServ code point (DSCP) and DSCP-IPv6 rewrite markers.

## Configuring Scheduler Buffer Size

You can configure the scheduler buffer size in three ways: as a temporal value, as a percentage, and as a remainder. On a single logical interface (MLPPP or a FRF.16 DLCI), each queue can have a different buffer size.

If you specify a temporal value, the queuing algorithm starts dropping packets when it queues more than a computed number of bytes. This number is computed by multiplying logical interface speed by the temporal value. For MLPPP bundles, logical interface speed is equal to the bundle bandwidth, which is the sum of constituent link speeds minus link-layer overhead. For MLFR FRF.16 DLCIs, logical interface speed is equal to bundle bandwidth multiplied by the DLCI shaping rate. In all cases, the maximum temporal value is limited to 200 milliseconds.

Buffer size percentages are implicitly converted into temporal values by multiplying the percentage by 200 milliseconds. For example, buffer size specified as **buffer-size percent 20** is the same as a 40-millisecond temporal delay. The link services IQ implementation guarantees 200 milliseconds of buffer delay for all interfaces with T1 and higher speeds. For slower interfaces, it guarantees one second of buffer delay.

The queuing algorithm evenly distributes leftover bandwidth among all queues that are configured with the **buffer-size remainder** statement. The queuing algorithm guarantees enough space in the transmit buffer for two MTU-sized packets.

## Configuring Scheduler Priority

The transmit priority of each queue is determined by the scheduler and the forwarding class. Each queue receives a guaranteed amount of bandwidth specified with the scheduler **transmit-rate** statement.

## Configuring Scheduler Shaping Rate

You use the shaping rate to set the percentage of total bundle bandwidth that is dedicated to a DLCI. For link services IQ DLCIs, only percentages are accepted, which allows adjustments in response to dynamic changes in bundle bandwidth—for example, when a link goes up or down. This means that absolute shaping rates are not supported on FRF.16 bundles. Absolute shaping rates are allowed for MLPPP and MLFR bundles only.

For scheduling between DLCIs in a MLFR FRF.16 bundle, you can configure a shaping rate for each DLCI. A shaping rate is expressed as a percentage of the aggregate bundle bandwidth. Shaping rate percentages for all DLCIs within a bundle can add up to 100 percent or less. Leftover bandwidth is distributed equally to DLCIs that do not have the **shaping-rate** statement included at the **[edit class-of-service interfaces lsq-fpc/pic/port:channel unit logical-unit-number]** hierarchy level. If none of the DLCIs in an MLFR FRF.16 bundle specify a DLCI scheduler, the total bandwidth is evenly divided across all DLCIs.



**NOTE:** For FRF.16 bundles on link services IQ interfaces, only shaping rates based on percentage are supported.

## Configuring Drop Profiles

You can configure random early detection (RED) on LSQ interfaces as in other CoS scenarios. To configure RED, include one or more drop profiles and attach them to a scheduler for a particular forwarding class. For more information about RED profiles, see the *Junos OS Class of Service Library for Routing Devices*.

The LSQ implementation performs tail RED. It supports a maximum of 256 drop profiles per PIC. Drop profiles are configurable on a per-queue, per-loss-priority, and per-TCP-bit basis.

You can attach scheduler maps with configured RED drop profiles to any LSQ logical interface: an MLPPP bundle, an FRF.15 bundle, or an FRF.16 DLCI. Different queues (forwarding classes) on the same logical interface can have different associated drop profiles.

The following example shows how to configure a RED profile on an LSQ interface:

```
[edit]
class-of-service {
  drop-profiles {
    drop-low {
      # Configure suitable drop profile for low loss priority
      ...
    }
  }
}
```

```

    }
    drop-high {
        # Configure suitable drop profile for high loss priority
        ...
    }
}
scheduler-maps {
    schedmap {
        # Best-effort queue will use be-scheduler
        # Other queues may use different schedulers
        forwarding-class be scheduler be-scheduler;
        ...
    }
}
schedulers {
    be-scheduler {
        # Configure two drop profiles for low and high loss priority
        drop-profile-map loss-priority low protocol any drop-profile drop-low;
        drop-profile-map loss-priority high protocol any drop-profile drop-high;
        # Other scheduler parameters (buffer-size, priority,
        # and transmit-rate) are already supported.
        ...
    }
}
interfaces {
    lsq-1/3/0.0 {
        # Attach a scheduler map (that includes RED drop profiles)
        # to a LSQ logical interface.
        scheduler-map schedmap;
    }
}
}

```



**NOTE:** The RED profiles should be applied only on the LSQ bundles and not on the egress links that constitute the bundle.

**Related  
Documentation**

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring Link Services and CoS on Services PICs on page 646](#)
- [Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces on page 633](#)
- [Link Services Configuration for Junos Interfaces](#)

## Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces

For link services IQ (**lsq-**) interfaces, you can specify fragmentation properties for specific forwarding classes. Traffic on each forwarding class can be either multilink encapsulated (fragmented and sequenced) or nonencapsulated (hashed with no fragmentation). By default, traffic in all forwarding classes is multilink encapsulated.

When you do not configure fragmentation properties for the queues on MLPPP interfaces, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number* fragment-threshold]** hierarchy level is the fragmentation threshold for all forwarding classes within the MLPPP interface. For MLFR FRF.16 interfaces, the fragmentation threshold you set at the **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options fragment-threshold]** hierarchy level is the fragmentation threshold for all forwarding classes within the MLFR FRF.16 interface.

If you do not set a maximum fragment size anywhere in the configuration, packets are still fragmented if they exceed the smallest maximum transmission unit (MTU) or maximum received reconstructed unit (MRRU) of all the links in the bundle. A nonencapsulated flow uses only one link. If the flow exceeds a single link, then the forwarding class must be multilink encapsulated, unless the packet size exceeds the MTU/MRRU.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the MRRU by including the **mrru** statement at the **[edit interfaces *lsq/fpc/pic/port* unit *logical-unit-number*]** or **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options]** hierarchy level. The MRRU is similar to the MTU, but is specific to link services interfaces. By default the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see [“Configuring MRRU on Multilink and Link Services Logical Interfaces” on page 1391](#).

To configure fragmentation properties on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
fragmentation-maps {
  map-name {
    forwarding-class class-name {
      (fragment-threshold bytes | no-fragmentation);
      multilink-class number;
    }
  }
}
```

To set a per-forwarding class fragmentation threshold, include the **fragment-threshold** statement in the fragmentation map. This statement sets the maximum size of each multilink fragment.

To set traffic on a queue to be nonencapsulated rather than multilink encapsulated, include the **no-fragmentation** statement in the fragmentation map. This statement specifies that an extra fragmentation header is not prepended to the packets received on this queue and that static link load balancing is used to ensure in-order packet delivery.

For a given forwarding class, you can include either the **fragment-threshold** or **no-fragmentation** statement; they are mutually exclusive.

You use the **multilink-class** statement to map a forwarding class into a multiclass MLPPP (MCML). For a given forwarding class, you can include either the **multilink-class** or **no-fragmentation** statement; they are mutually exclusive. For more information about MCML, see [“Configuring Multiclass MLPPP on LSQ Interfaces” on page 636](#).

To associate a fragmentation map with a multilink PPP interface or MLFR FRF.16 DLCI, include the **fragmentation-map** statement at the **[edit class-of-service interfaces interface-name unit logical-unit-number]** hierarchy level:

```
[edit class-of-service interfaces]
lsq-fpc/pic/port {
  unit logical-unit-number { # Multilink PPP
    fragmentation-map map-name;
  }
lsq-fpc/pic/port:channel { # MLFR FRF.16
  unit logical-unit-number {
    fragmentation-map map-name;
  }
}
```

For configuration examples, see the following topics:

- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using MLPPP on page 649](#)
- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using FRF.16 on page 655](#)
- [Configuring LSQ Interfaces for Single Fractional T1 or El Interfaces Using MLPPP and LFI on page 660](#)
- [Configuring LSQ Interfaces for Single Fractional T1 or El Interfaces Using FRF.12 on page 665](#)
- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using FRF.15 on page 672](#)
- [Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP on page 673](#)
- [Configuring LSQ Interfaces as T3 or OC3 Bundles Using FRF.12 on page 675](#)
- [Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP on page 677](#)

For Link Services PIC link services (**ls-**) interfaces, fragmentation maps are not supported. Instead, you enable LFI by including the **interleave-fragments** statement at the **[edit interfaces interface-name unit logical-unit-number]** hierarchy level. For more information, see “Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces” on page 1394.

#### Related Documentation

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring Link Services and CoS on Services PICs on page 646](#)
- [Configuring CoS Scheduling Queues on Logical LSQ Interfaces on page 630](#)
- [Link Services Configuration for Junos Interfaces](#)

## Reserving Bundle Bandwidth for Link-Layer Overhead on LSQ Interfaces

Link-layer overhead can cause packet drops on constituent links because of bit stuffing on serial links. Bit stuffing is used to prevent data from being interpreted as control information.

By default, 4 percent of the total bundle bandwidth is set aside for link-layer overhead. In most network environments, the average link-layer overhead is 1.6 percent. Therefore, we recommend 4 percent as a safeguard. For more information, see RFC 4814, *Hash and Stuffing: Overlooked Factors in Network Device Benchmarking*.

For link services IQ (**lsq-**) interfaces, you can configure the percentage of bundle bandwidth to be set aside for link-layer overhead. To do this, include the **link-layer-overhead** statement:

```
link-layer-overhead percent;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* **mlfr-uni-nni-bundle-options**]
- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

You can configure the value to be from 0 percent through 50 percent.

**Related  
Documentation**

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Oversubscribing Interface Bandwidth on LSQ Interfaces on page 638](#)
- [Configuring Guaranteed Minimum Rate on LSQ Interfaces on page 643](#)
- [Link Services Configuration for Junos Interfaces](#)

---

## Configuring Multiclass MLPPP on LSQ Interfaces

---

For link services IQ (**lsq-**) interfaces with MLPPP encapsulation, you can configure multiclass MLPPP (MCML). If you do not configure MCML, fragments from different classes cannot be interleaved. All fragments for a single packet must be sent before the fragments from another packet are sent. Nonfragmented packets can be interleaved between fragments of another packet to reduce latency seen by nonfragmented packets. In effect, latency-sensitive traffic is encapsulated as regular PPP traffic, and bulk traffic is encapsulated as multilink traffic. This model works as long as there is a single class of latency-sensitive traffic, and there is no high-priority traffic that takes precedence over latency-sensitive traffic. This approach to LFI, used on the Link Services PIC, supports only two levels of traffic priority, which is not sufficient to carry the four-to-eight forwarding classes that are supported by M Series and T Series routers. For more information about the Link Services PIC support of LFI, see “[Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces](#)” on page 1394.

For link services IQ interfaces only, you can configure MCML, as defined in RFC 2686, *The Multi-Class Extension to Multi-Link PPP*. MCML makes it possible to have multiple classes of latency-sensitive traffic that are carried over a single multilink bundle with bulk traffic. In effect, MCML allows different classes of traffic to have different latency guarantees. With MCML, you can map each forwarding class into a separate multilink class, thus preserving priority and latency guarantees.



**NOTE:** Configuring both LFI and MCML on the same bundle is not necessary, nor is it supported, because multiclass MLPPP represents a superset of functionality. When you configure multiclass MLPPP, LFI is automatically enabled.

The Junos OS implementation of MCML does not support compression of common header bytes, which is referred to in RFC 2686 as “prefix elision.”

MCML greatly simplifies packet ordering issues that occur when multiple links are used. Without MCML, all voice traffic belonging to a single flow is hashed to a single link to avoid packet ordering issues. With MCML, you can assign voice traffic to a high-priority class, and you can use multiple links. For more information about voice services support on link services IQ interfaces (**lsq**), see [“Configuring Services Interfaces for Voice Services” on page 696](#).

To configure MCML on a link services IQ interface, you must specify how many multilink classes should be negotiated when a link joins the bundle, and you must specify the mapping of a forwarding class into an MCML class.

To specify how many multilink classes should be negotiated when a link joins the bundle, include the **multilink-max-classes** statement:

```
multilink-max-classes number;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

The number of multilink classes can be 1 through 8. The number of multilink classes for each forwarding class must not exceed the number of multilink classes to be negotiated.

To specify the mapping of a forwarding class into a MCML class, include the **multilink-class** statement at the [edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*] hierarchy level:

```
[edit class-of-service fragmentation-maps map-name forwarding-class class-name]
multilink-class number;
```

The multilink class index number can be 0 through 7. The **multilink-class** statement and **no-fragmentation** statements are mutually exclusive.

To view the number of multilink classes negotiated, issue the **show interfaces lsq-fpc/port.port.logical-unit-number detail** command.

#### Related Documentation

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using MLPPP on page 649](#)
- [Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP on page 677](#)

- [Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP on page 673](#)
- [Link Services Configuration for Junos Interfaces](#)

---

## Oversubscribing Interface Bandwidth on LSQ Interfaces

---

The term *oversubscribing interface bandwidth* means configuring shaping rates (peak information rates [PIRs]) so that their sum exceeds the interface bandwidth.

On Channelized IQ PICs, Gigabit Ethernet IQ PICs, and FRF.16 link services IQ (**lsq-**) interfaces on AS and Multiservices PICs, you can oversubscribe interface bandwidth. The logical interfaces (and DLCIs within an FRF.16 bundle) can be oversubscribed when there is leftover bandwidth. The oversubscription is limited to the configured PIR. Any unused bandwidth is distributed equally among oversubscribed logical interfaces or DLCIs.

For networks that are not likely to experience congestion, oversubscribing interface bandwidth improves network utilization, thereby allowing more customers to be provisioned on a single interface. If the actual data traffic does not exceed the interface bandwidth, oversubscription allows you to sell more bandwidth than the interface can support.

We recommend avoiding oversubscription in networks that are likely to experience congestion. Be careful not to oversubscribe a service by too much, because this can cause degradation in the performance of the router during congestion. When you configure oversubscription, some output queues can be starved if the actual data traffic exceeds the physical interface bandwidth. You can prevent degradation by using statistical multiplexing to ensure that the actual data traffic does not exceed the interface bandwidth.



**NOTE:** You cannot oversubscribe interface bandwidth when you configure traffic shaping using the method described in *Applying Scheduler Maps and Shaping Rate to DLCIs and VLANs*.

---

When configuring oversubscription for FRF.16 bundle interfaces, you can assign traffic control profiles that apply on a physical interface basis. When you apply traffic control profiles to FRF.16 bundles at the *logical* interface level, member link interface bandwidth is underutilized when there is a small proportion of traffic or no traffic at all on an individual DLCI. Support for traffic control features on the FRF.16 bundle physical interface level addresses this limitation.

To configure oversubscription of an interface, perform the following steps:

1. Include the **shaping-rate** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

```
[edit class-of-service traffic-control-profiles profile-name]  
shaping-rate (percent percentage | rate);
```



**NOTE:** When configuring oversubscription for FRF.16 bundle interfaces on a physical interface basis, you *must* specify **shaping-rate** as a percentage.

On LSQ interfaces, you can configure the shaping rate as a percentage.

On IQ and IQ2 interfaces, you can configure the shaping rate as an absolute rate from 1000 through 160,000,000,000 bits per second.

Alternatively, you can configure a shaping rate for a logical interface and oversubscribe the physical interface by including the **shaping-rate** statement at the [edit **class-of-service interfaces interface-name unit logical-unit-number**] hierarchy level. However, with this configuration approach, you cannot independently control the delay-buffer rate, as described in Step 2.



**NOTE:** For channelized and Gigabit Ethernet IQ interfaces, the **shaping-rate** and **guaranteed-rate** statements are mutually exclusive. You cannot configure some logical interfaces to use a shaping rate and others to use a guaranteed rate. This means there are no service guarantees when you configure a PIR. For these interfaces, you can configure either a PIR or a committed information rate (CIR), but not both.

This restriction does not apply to Gigabit Ethernet IQ2 PICs or link services IQ (LSQ) interfaces on AS or Multiservices PICs. For LSQ and Gigabit Ethernet IQ2 interfaces, you can configure both a PIR and a CIR on an interface. For more information about CIRs, see [“Configuring Guaranteed Minimum Rate on LSQ Interfaces” on page 643](#).

2. Optionally, you can base the delay buffer calculation on a delay-buffer rate. To do this, include the **delay-buffer-rate** statement at the [edit **class-of-service traffic-control-profiles profile-name**] hierarchy level:



**NOTE:** When configuring oversubscription for FRF.16 bundle interfaces on a physical interface basis, you *must* specify **delay-buffer-rate** as a percentage.

```
[edit class-of-service traffic-control-profiles profile-name]
delay-buffer-rate (percent percentage | rate);
```

The delay-buffer rate overrides the shaping rate as the basis for the delay-buffer calculation. In other words, the shaping rate or scaled shaping rate is used for delay-buffer calculations only when the delay-buffer rate is not configured.

For LSQ interfaces, if you do not configure a delay-buffer rate, the guaranteed rate (CIR) is used to assign buffers. If you do not configure a guaranteed rate, the shaping rate (PIR) is used in the undersubscribed case, and the scaled shaping rate is used in the oversubscribed case.

On LSQ interfaces, you can configure the delay-buffer rate as a percentage.

On IQ and IQ2 interfaces, you can configure the delay-buffer rate as an absolute rate from 1000 through 160,000,000,000 bits per second.

The actual delay buffer is based on the calculations described in the *Junos OS Class of Service Library for Routing Devices*. For an example showing how the delay-buffer rates are applied, see [“Examples: Oversubscribing an LSQ Interface” on page 641](#).

Configuring large buffers on relatively low-speed links can cause packet aging. To help prevent this problem, the software requires that the sum of the delay-buffer rates be less than or equal to the port speed.

This restriction does not eliminate the possibility of packet aging, so you should be cautious when using the **delay-buffer-rate** statement. Though some amount of extra buffering might be desirable for burst absorption, delay-buffer rates should not far exceed the service rate of the logical interface.

If you configure delay-buffer rates so that the sum exceeds the port speed, the configured delay-buffer rate is not implemented for the last logical interface that you configure. Instead, that logical interface receives a delay-buffer rate of zero, and a warning message is displayed in the CLI. If bandwidth becomes available (because another logical interface is deleted or deactivated, or the port speed is increased), the configured delay-buffer-rate is reevaluated and implemented if possible.

If you do not configure a delay-buffer rate or a guaranteed rate, the logical interface receives a delay-buffer rate in proportion to the shaping rate and the remaining delay-buffer rate available. In other words, the delay-buffer rate for each logical interface with no configured delay-buffer rate is equal to:

$$(\text{remaining delay-buffer rate} * \text{shaping rate}) / (\text{sum of shaping rates})$$

The remaining delay-buffer rate is equal to:

$$(\text{interface speed}) - (\text{sum of configured delay-buffer rates})$$

3. To assign a scheduler map to the logical interface, include the **scheduler-map** statement at the **[edit class-of-service traffic-control-profiles profile-name]** hierarchy level:

```
[edit class-of-service traffic-control-profiles profile-name]
  scheduler-map map-name;
```

For information about configuring schedulers and scheduler maps, see the *Junos OS Class of Service Library for Routing Devices*.

4. Optionally, you can enable large buffer sizes to be configured. To do this, include the **q-pic-large-buffer** statement at the **[edit chassis fpc slot-number pic pic-number]** hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
  q-pic-large-buffer;
```

If you do not include this statement, the delay-buffer size is more restricted.

We recommend restricted buffers for delay-sensitive traffic, such as voice traffic. For more information, see the *Junos OS Class of Service Library for Routing Devices*.

5. To enable scheduling on logical interfaces, include the **per-unit-scheduler** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name ]
per-unit-scheduler;
```

When you include this statement, the maximum number of VLANs supported is 768 on a single-port Gigabit Ethernet IQ PIC. On a two-port Gigabit Ethernet IQ PIC, the maximum number is 384.

6. To enable scheduling for FRF.16 bundles physical interfaces, include the **no-per-unit-scheduler** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
no-per-unit-scheduler;
```

7. To apply the traffic-scheduling profile to the logical interface, include the **output-traffic-control-profile** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]** hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
output-traffic-control-profile profile-name;
```

You cannot include the **output-traffic-control-profile** statement in the configuration if any of the following statements are included in the logical interface configuration: **scheduler-map**, **shaping-rate**, **adaptive-shaper**, or **virtual-channel-group**.

For a table that shows how the bandwidth and delay buffer are allocated in various configurations, see the *Junos OS Class of Service Library for Routing Devices*.

## Examples: Oversubscribing an LSQ Interface

### Oversubscribing an LSQ Interface with Scheduling Based on the Logical Interface

Apply a traffic-control profile to a logical interface representing a DLCI on an FRF.16 bundle.

```
interfaces {
  lsq-1/3/0:0 {
    per-unit-scheduler;
    unit 0 {
      dlci 100;
    }
    unit 1 {
      dlci 200;
    }
  }
}
class-of-service {
  traffic-control-profiles {
    tc_0 {
      shaping-rate percent 100;
      guaranteed-rate percent 60;
      delay-buffer-rate percent 80;
    }
    tc_1 {
      shaping-rate percent 80;
      guaranteed-rate percent 40;
    }
  }
}
```

```

    }
    interfaces {
      lsq-1/3/0 {
        unit 0 {
          output-traffic-control-profile tc_0;
        }
        unit 1 {
          output-traffic-control-profile tc_1;
        }
      }
    }
  }
}

```

#### Oversubscribing an LSQ Interface with Scheduling Based on the Physical Interface

Apply a traffic-control profile to the physical interface representing an FRF.16 bundle:

```

interfaces {
  lsq-0/2/0:0 {
    no-per-unit-scheduler;
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
      dlci 100;
      family inet {
        address 18.18.18.2/24;
      }
    }
  }
}

class-of-service {
  traffic-control-profiles {
    rlsq_tc {
      scheduler-map rlsq;
      shaping-rate percent 60;
      delay-buffer-rate percent 10;
    }
  }
  interfaces {
    lsq-0/2/0:0 {
      output-traffic-control-profile rlsq_tc;
    }
  }
}

scheduler-maps {
  rlsq {
    forwarding-class best-effort scheduler rlsq_scheduler;
    forwarding-class expedited-forwarding scheduler rlsq_scheduler1;
  }
}

schedulers {
  rlsq_scheduler {
    transmit-rate percent 20;
    priority low;
  }
  rlsq_scheduler1 {
    transmit-rate percent 40;
    priority high;
  }
}

```

- Related Documentation**
- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
  - [Reserving Bundle Bandwidth for Link-Layer Overhead on LSQ Interfaces on page 635](#)
  - [Configuring Guaranteed Minimum Rate on LSQ Interfaces on page 643](#)
  - [Link Services Configuration for Junos Interfaces](#)

## Configuring Guaranteed Minimum Rate on LSQ Interfaces

On Gigabit Ethernet IQ PICs, Channelized IQ PICs, and FRF.16 link services IQ (LSQ) interfaces on AS and Multiservices PICs, you can configure guaranteed bandwidth, also known as a committed information rate (CIR). This allows you to specify a guaranteed rate for each logical interface. The guaranteed rate is a minimum. If excess physical interface bandwidth is available for use, the logical interface receives more than the guaranteed rate provisioned for the interface.

You cannot provision the sum of the guaranteed rates to be more than the physical interface bandwidth, or the bundle bandwidth for LSQ interfaces. If the sum of the guaranteed rates exceeds the interface or bundle bandwidth, the commit operation does not fail, but the software automatically decreases the rates so that the sum of the guaranteed rates is equal to the available bundle bandwidth.

To configure a guaranteed minimum rate, perform the following steps:

1. Include the **guaranteed-rate** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

```
[edit class-of-service traffic-control-profiles profile-name]
  guaranteed-rate (percent percentage | rate);
```

On LSQ interfaces, you can configure the guaranteed rate as a percentage.

On IQ and IQ2 interfaces, you can configure the guaranteed rate as an absolute rate from 1000 through 160,000,000,000 bits per second.



**NOTE:** For channelized and Gigabit Ethernet IQ interfaces, the **shaping-rate** and **guaranteed-rate** statements are mutually exclusive. You cannot configure some logical interfaces to use a shaping rate and others to use a guaranteed rate. This means there are no service guarantees when you configure a PIR. For these interfaces, you can configure either a PIR or a committed information rate (CIR), but not both.

This restriction does not apply to Gigabit Ethernet IQ2 PICs or link services IQ (LSQ) interfaces on AS or Multiservices PICs. For LSQ and Gigabit Ethernet IQ2 interfaces, you can configure both a PIR and a CIR on an interface. For more information about CIRs, see the *Junos OS Class of Service Library for Routing Devices*.

2. Optionally, you can base the delay buffer calculation on a delay-buffer rate. To do this, include the **delay-buffer-rate** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

```
[edit class-of-service traffic-control-profiles profile-name]  
  delay-buffer-rate (percent percentage | rate);
```

On LSQ interfaces, you can configure the delay-buffer rate as a percentage.

On IQ and IQ2 interfaces, you can configure the delay-buffer rate as an absolute rate from 1000 through 160,000,000,000 bits per second.

The actual delay buffer is based on the calculations described in tables in the *Junos OS Class of Service Library for Routing Devices*. For an example showing how the delay-buffer rates are applied, see [“Example: Configuring Guaranteed Minimum Rate” on page 645](#).

If you do not include the **delay-buffer-rate** statement, the delay-buffer calculation is based on the guaranteed rate, the shaping rate if no guaranteed rate is configured, or the scaled shaping rate if the interface is oversubscribed.

If you do not specify a shaping rate or a guaranteed rate, the logical interface receives a minimal delay-buffer rate and minimal bandwidth equal to 4 MTU-sized packets.

You can configure a rate for the delay buffer that is higher than the guaranteed rate. This can be useful when the traffic flow might not require much bandwidth in general, but in some cases can be bursty and therefore needs a large buffer.

Configuring large buffers on relatively low-speed links can cause packet aging. To help prevent this problem, the software requires that the sum of the delay-buffer rates be less than or equal to the port speed. This restriction does not eliminate the possibility of packet aging, so you should be cautious when using the **delay-buffer-rate** statement. Though some amount of extra buffering might be desirable for burst absorption, delay-buffer rates should not far exceed the service rate of the logical interface.

If you configure delay-buffer rates so that the sum exceeds the port speed, the configured delay-buffer rate is not implemented for the last logical interface that you configure. Instead, that logical interface receives a delay-buffer rate of 0, and a warning message is displayed in the CLI. If bandwidth becomes available (because another logical interface is deleted or deactivated, or the port speed is increased), the configured delay-buffer-rate is reevaluated and implemented if possible.

If the guaranteed rate of a logical interface cannot be implemented, that logical interface receives a delay-buffer rate of 0, even if the configured delay-buffer rate is within the interface speed. If at a later time the guaranteed rate of the logical interface can be met, the configured delay-buffer rate is reevaluated and if the delay-buffer rate is within the remaining bandwidth, it is implemented.

If any logical interface has a configured guaranteed rate, all other logical interfaces on that port that do not have a guaranteed rate configured receive a delay-buffer rate of 0. This is because the absence of a guaranteed rate configuration corresponds to a guaranteed rate of 0 and, consequently, a delay-buffer rate of 0.

3. To assign a scheduler map to the logical interface, include the **scheduler-map** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

```
[edit class-of-service traffic-control-profiles profile-name]
  scheduler-map map-name;
```

For information about configuring schedulers and scheduler maps, see the *Junos OS Class of Service Library for Routing Devices*.

4. To enable large buffer sizes to be configured, include the **q-pic-large-buffer** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
  q-pic-large-buffer;
```

If you do not include this statement, the delay-buffer size is more restricted. For more information, see the *Junos OS Class of Service Library for Routing Devices*.

5. To enable scheduling on logical interfaces, include the **per-unit-scheduler** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name ]
  per-unit-scheduler;
```

When you include this statement, the maximum number of VLANs supported is 767 on a single-port Gigabit Ethernet IQ PIC. On a two-port Gigabit Ethernet IQ PIC, the maximum number is 383.

6. To apply the traffic-scheduling profile to the logical interface, include the **output-traffic-control-profile** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]** hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
  output-traffic-control-profile profile-name;
```

## Example: Configuring Guaranteed Minimum Rate

Two logical interface units, **0** and **1**, are provisioned with a guaranteed minimum of 750 Kbps and 500 Kbps, respectively. For logical unit **1**, the delay buffer is based on the guaranteed rate setting. For logical unit **0**, a delay-buffer rate of 500 Kbps is specified. The actual delay buffers allocated to each logical interface are 2 seconds of 500 Kbps. The 2-second value is based on the following calculation:

$$\text{delay-buffer-rate} < [8 \times 64 \text{ Kbps}]: 2 \text{ seconds of delay-buffer-rate}$$

For more information about this calculation, see the *Junos OS Class of Service Library for Routing Devices*.

```
chassis {
  fpc 3 {
    pic 0 {
      q-pic-large-buffer;
    }
  }
}
interfaces {
```

```
t1-3/0/1 {
  per-unit-scheduler;
}
}
class-of-service {
  traffic-control-profiles {
    tc-profile3 {
      guaranteed-rate 750k;
      scheduler-map sched-map3;
      delay-buffer-rate 500k; # 500 Kbps is less than 8 x 64 Kbps
    }
    tc-profile4 {
      guaranteed-rate 500k; # 500 Kbps is less than 8 x 64 Kbps
      scheduler-map sched-map4;
    }
  }
}
interface t1-3/0/1 {
  unit 0 {
    output-traffic-control-profile tc-profile3;
  }
  unit 1 {
    output-traffic-control-profile tc-profile4;
  }
}
}
```

**Related Documentation**

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Reserving Bundle Bandwidth for Link-Layer Overhead on LSQ Interfaces on page 635](#)
- [Oversubscribing Interface Bandwidth on LSQ Interfaces on page 638](#)
- [Link Services Configuration for Junos Interfaces](#)

---

## Configuring Link Services and CoS on Services PICs

---

To configure link services and CoS on an AS or Multiservices PIC, you must perform the following steps:

1. Enable the Layer 2 service package. You enable service packages per PIC, not per port. When you enable the Layer 2 service package, the entire PIC uses the configured package. To enable the Layer 2 service package, include the **service-package** statement at the **[edit chassis fpc slot-number pic pic-number adaptive-services]** hierarchy level, and specify **layer-2**:

```
[edit chassis fpc slot-number pic pic-number adaptive-services]
service-package layer-2;
```

For more information about AS or Multiservices PIC service packages, see [“Enabling Service Packages” on page 41](#) and [“Layer 2 Service Package Capabilities and Interfaces” on page 616](#).

2. Configure a multilink PPP or FRF.16 bundle by combining constituent links into a virtual link, or bundle.

### Configuring an MLPPP Bundle

To configure an MLPPP bundle, configure constituent links and bundle properties by including the following statements in the configuration:

```
[edit interfaces interface-name unit logical-unit-number]
encapsulation ppp;
family mlppp {
    bundle lsq-fpc/pic/port.logical-unit-number;
}
[edit interfaces lsq-fpc/pic/port unit logical-unit-number]
drop-timeout milliseconds;
encapsulation multilink-ppp;
fragment-threshold bytes;
link-layer-overhead percent;
minimum-links number;
mrru bytes;
short-sequence;
family inet {
    address address;
}
```

For more information about these statements, see the *Link and Multilink Properties*.

### Configuring an MLFR FRF.16 Bundle

To configure an MLFR FRF.16 bundle, configure constituent links and bundle properties by including the following statements in the configuration:

```
[edit chassis fpc slot-number pic slot-number]
mlfr-uni-nni-bundles number;
[edit interfaces interface-name ]
encapsulation multilink-frame-relay-uni-nni;
unit logical-unit-number {
    family mlfr-uni-nni {
        bundle lsq-fpc/pic/port:channel;
    }
}
```

For more information about the **mlfr-uni-nni-bundles** statement, see the *Junos OS Administration Library for Routing Devices*. MLFR FRF.16 uses channels as logical units.

For MLFR FRF.16, you must configure one end as data circuit-terminating equipment (DCE) by including the following statements at the **[edit interfaces *lsq-fpc/pic/port:channel*]** hierarchy level.

```
encapsulation multilink-frame-relay-uni-nni;
dce;
mlfr-uni-nni-options {
    acknowledge-retries number;
    acknowledge-timer milliseconds;
    action-red-differential-delay (disable-tx | remove-link);
    drop-timeout milliseconds;
    fragment-threshold bytes;
    hello-timer milliseconds;
    link-layer-overhead percent;
    lmi-type (ansi | itu);
    minimum-links number;
```

```

    mrru bytes;
    n391 number;
    n392 number;
    n393 number;
    red-differential-delay milliseconds;
    t391 number;
    t392 number;
    yellow-differential-delay milliseconds;
  }
  unit logical-unit-number {
    dlci dlci-identifier;
    family inet {
      address address;
    }
  }
}

```

For more information about MLFR UNI NNI properties, see *Link and Multilink Properties*.

3. To configure CoS components for each multilink bundle, enable per-unit scheduling on the interface, configure a scheduler map, apply the scheduler to each queue, configure a fragmentation map, and apply the fragmentation map to each bundle. Include the following statements:

```

[edit interfaces]
lsq-fpc/pic/port {
  per-unit-scheduler; # Enables per-unit scheduling on the bundle
}
[edit class-of-service]
interfaces {
  lsq-fpc/pic/port { # Multilink PPP
    unit logical-unit-number {
      scheduler-map map-name; # Applies scheduler map to each queue
    }
  }
}
lsq-fpc/pic/port:channel { # MLFR FRF.16
  unit logical-unit-number {
    # Scheduler map provides scheduling information for
    # the queues within a single DLCI.
    scheduler-map map-name;
    shaping-rate percent percent;
  }
}
forwarding-classes {
  queue queue-number class-name priority (high | low);
}
scheduler-maps {
  map-name {
    forwarding-class class-name scheduler scheduler-name;
  }
}
schedulers {
  scheduler-name {
    buffer-size (percent percentage | remainder | temporal microseconds);
    priority priority-level;
    transmit-rate (percent percentage | rate | remainder) <exact>;
  }
}

```

```

fragmentation-maps {
  map-name {
    forwarding-class class-name {
      fragment-threshold bytes;
      no-fragmentation;
    }
  }
}

```

Associate a fragmentation map with a multilink PPP interface or MLFR FRF.16 DLCI by including the following statements at the **[edit class-of-service]** hierarchy level:

```

interfaces {
  lsq-fpc/pic/port {
    unit logical-unit-number { # Multilink PPP
      fragmentation-map map-name;
    }
  }
  lsq-fpc/pic/port:channel { # MLFR FRF.16
    unit logical-unit-number {
      fragmentation-map map-name;
    }
  }
}

```

#### Related Documentation

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS on page 618](#)
- [Configuring LSQ Interface Redundancy in a Single Router Using SONET APS on page 620](#)
- [Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621](#)
- [Link Services Configuration for Junos Interfaces](#)

## Configuring LSQ Interfaces as NxT1 or Nx E1 Bundles Using MLPPP

To configure an NxT1 bundle using MLPPP, you aggregate *N* different T1 links into a bundle. The NxT1 bundle is called a logical interface, because it can represent, for example, a routing adjacency. To aggregate T1 links into an MLPPP bundle, include the **bundle** statement at the **[edit interfaces t1-fpc/pic/port unit logical-unit-number family mlppp]** hierarchy level:

```

[edit interfaces t1-fpc/pic/port unit logical-unit-number family mlppp]
bundle lsq-fpc/pic/port.logical-unit-number;

```



**NOTE:** Link services IQ interfaces support both T1 and E1 physical interfaces. These instructions apply to T1 interfaces, but the configuration for E1 interfaces is similar.

To configure the link services IQ interface properties, include the following statements at the **[edit interfaces lsq-fpc/pic/port unit logical-unit-number]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port unit logical-unit-number]
drop-timeout milliseconds;
encapsulation multilink-ppp;
fragment-threshold bytes;
link-layer-overhead percent;
minimum-links number;
mrru bytes;
short-sequence;
family inet {
    address address;
}
```

The logical link services IQ interface represents the MLPPP bundle. For the MLPPP bundle, there are four associated queues on M Series routers and eight associated queues on M320 and T Series routers. A scheduler removes packets from the queues according to a scheduling policy. Typically, you designate one queue to have strict priority, and the remaining queues are serviced in proportion to weights you configure.

For MLPPP, assign a single scheduler map to the link services IQ interface (**lsq**) and to each constituent link. The default schedulers for M Series and T Series routers, which assign 95, 0, 0, and 5 percent bandwidth for the transmission rate and buffer size of queues 0, 1, 2, and 3, are not adequate when you configure LFI or multiclass traffic. Therefore, for MLPPP, you should configure a single scheduler with nonzero percent transmission rates and buffer sizes for queues 0 through 3, and assign this scheduler to the link services IQ interface (**lsq**) and to each constituent link, as shown in [“Example: Configuring an LSQ Interface as an NxTI Bundle Using MLPPP”](#) on page 652.



**NOTE:** For M320 and T Series routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

If the member link belonging to one MLPP, MLFR, or MFR bundle interface is moved to another bundle interface, or the links are swapped between two bundle interfaces, a commit is required between the delete and add operations to ensure that the configuration is applied correctly.

If the bundle has more than one link, you must include the **per-unit-scheduler** statement at the **[edit interfaces lsq-fpc/pic/port]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port]
per-unit-scheduler;
```

To configure and apply the scheduling policy, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
interfaces {
    t1-fpc/pic/port unit logical-unit-number {
        scheduler-map map-name;
    }
}
forwarding-classes {
```

```

    queue queue-number class-name;
  }
  scheduler-maps {
    map-name {
      forwarding-class class-name scheduler scheduler-name;
    }
  }
  schedulers {
    scheduler-name {
      buffer-size (percent percentage | remainder | temporal microseconds);
      priority priority-level;
      transmit-rate (rate | percent percentage | remainder) <exact>;
    }
  }
}

```

For link services IQ interfaces, a strict-high-priority queue might starve the other three queues because traffic in a strict-high priority queue is transmitted before any other queue is serviced. This implementation is unlike the standard Junos CoS implementation in which a strict-high-priority queue does round-robin with high-priority queues, as described in the *Junos OS Class of Service Library for Routing Devices*.

After the scheduler removes a packet from a queue, a certain action is taken. The action depends on whether the packet came from a multilink encapsulated queue (fragmented and sequenced) or a nonencapsulated queue (hashed with no fragmentation). Each queue can be designated as either multilink encapsulated or nonencapsulated, independently of the other. By default, traffic in all forwarding classes is multilink encapsulated. To configure packet fragmentation handling on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```

fragmentation-maps {
  map-name {
    forwarding-class class-name {
      fragment-threshold bytes;
      multilink-class number;
      no-fragmentation;
    }
  }
}

```

For *NxT1* bundles using MLPPP, the byte-wise load balancing used in multilink-encapsulated queues is superior to the flow-wise load balancing used in nonencapsulated queues. All other considerations are equal. Therefore, we recommend that you configure all queues to be multilink encapsulated. You do this by including the **fragment-threshold** statement in the configuration. If you choose to set traffic on a queue to be nonencapsulated rather than multilink encapsulated, include the **no-fragmentation** statement in the fragmentation map. You use the **multilink-class** statement to map a forwarding class into a multiclass MLPPP (MCML). For more information about MCML, see [“Configuring Multiclass MLPPP on LSQ Interfaces” on page 636](#). For more information about fragmentation maps, see [“Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces” on page 633](#).

When a packet is removed from a multilink-encapsulated queue, the software gives the packet an MLPPP header. The MLPPP header contains a sequence number field, which

is filled with the next available sequence number from a counter. The software then places the packet on one of the  $N$  different T1 links. The link is chosen on a packet-by-packet basis to balance the load across the various T1 links.

If the packet exceeds the minimum link MTU, or if a queue has a fragment threshold configured at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level, the software splits the packet into two or more fragments, which are assigned consecutive multilink sequence numbers. The outgoing link for each fragment is selected independently of all other fragments.

If you do not include the **fragment-threshold** statement in the fragmentation map, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest MTU of all the links in the bundle.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the maximum received reconstructed unit (MRRU) by including the **mrru** statement at the **[edit interfaces *lsq/fpc/pic/port* unit *logical-unit-number*]** hierarchy level. The MRRU is similar to the MTU, but is specific to link services interfaces. By default the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see [“Configuring MRRU on Multilink and Link Services Logical Interfaces” on page 1391](#).

When a packet is removed from a nonencapsulated queue, it is transmitted with a plain PPP header. Because there is no MLPPP header, there is no sequence number information. Therefore, the software must take special measures to avoid packet reordering. To avoid packet reordering, the software places the packet on one of the  $N$  different T1 links. The link is determined by hashing the values in the header. For IP, the software computes the hash based on source address, destination address, and IP protocol. For MPLS, the software computes the hash based on up to five MPLS labels, or four MPLS labels and the IP header.

For UDP and TCP the software computes the hash based on the source and destination ports, as well as source and destination IP addresses. This guarantees that all packets belonging to the same TCP/UDP flow always pass through the same T1 link, and therefore cannot be reordered. However, it does not guarantee that the load on the various T1 links is balanced. If there are many flows, the load is usually balanced.

The  $N$  different T1 interfaces link to another router, which can be from Juniper Networks or another vendor. The router at the far end gathers packets from all the T1 links. If a packet has an MLPPP header, the sequence number field is used to put the packet back into sequence number order. If the packet has a plain PPP header, the software accepts the packet in the order in which it arrives and makes no attempt to reassemble or reorder the packet.

### Example: Configuring an LSQ Interface as an NxT1 Bundle Using MLPPP

```
[edit chassis]
fpc 1 {
  pic 3 {
    adaptive-services {
```

```

        service-package layer-2;
    }
}
[edit interfaces]
t1-0/0/0 {
    encapsulation ppp;
    unit 0 {
        family mlppp {
            bundle lsq-1/3/0.1; # This adds t1-0/0/0 to the specified bundle.
        }
    }
}
t1-0/0/1 {
    encapsulation ppp;
    unit 0 {
        family mlppp {
            bundle lsq-1/3/0.1;
        }
    }
}
lsq-1/3/0 {
    unit 1 { # This is the virtual link that concatenates multiple T1s.
        encapsulation multilink-ppp;
        drop-timeout 1000;
        fragment-threshold 128;
        link-layer-overhead 0.5;
        minimum-links 2;
        mrru 4500;
        short-sequence;
        family inet {
            address 10.2.3.4/24;
        }
    }
}
[edit interfaces]
lsq-1/3/0 {
    per-unit-scheduler;
}
[edit class-of-service]
interfaces {
    lsq-1/3/0 { # multilink PPP constituent link
        unit 0 {
            scheduler-map sched-map1;
        }
    }
    t1-0/0/0 { # multilink PPP constituent link
        unit 0 {
            scheduler-map sched-map1;
        }
    }
    t1-0/0/1 { # multilink PPP constituent link
        unit 0 {
            scheduler-map sched-map1;
        }
    }
    forwarding-classes {
        queue 0 be;
        queue 1 ef;
    }
}

```

```
    queue 2 af;
    queue 3 nc;
}
scheduler-maps {
  sched-map1 {
    forwarding-class af scheduler af-scheduler;
    forwarding-class be scheduler be-scheduler;
    forwarding-class ef scheduler ef-scheduler;
    forwarding-class nc scheduler nc-scheduler;
  }
}
schedulers {
  af-scheduler {
    transmit-rate percent 30;
    buffer-size percent 30;
    priority low;
  }
  be-scheduler {
    transmit-rate percent 25;
    buffer-size percent 25;
    priority low;
  }
  ef-scheduler {
    transmit-rate percent 40;
    buffer-size percent 40;
    priority strict-high; # voice queue
  }
  nc-scheduler {
    transmit-rate percent 5;
    buffer-size percent 5;
    priority high;
  }
}
fragmentation-maps {
  fragmap-1 {
    forwarding-class be {
      fragment-threshold 180;
    }
    forwarding-class ef {
      fragment-threshold 100;
    }
  }
}
[edit interfaces]
lsq-1/3/0 {
  unit 0 {
    fragmentation-map fragmap-1;
  }
}
```

**Related Documentation**

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using FRF.16 on page 655](#)
- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using FRF.15 on page 672](#)
- [Link Services Configuration for Junos Interfaces](#)

## Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.16

To configure an NxT1 bundle using FRF.16, you aggregate *N* different T1 links into a bundle. The NxT1 bundle carries a potentially large number of Frame Relay PVCs, identified by their DLCIs. Each DLCI is called a logical interface, because it can represent, for example, a routing adjacency.

To aggregate T1 links into an FRF.16 bundle, include the **mlfr-uni-nni-bundles** statement at the **[edit chassis fpc slot-number pic slot-number]** hierarchy level and include the **bundle** statement at the **[edit interfaces t1-fpc/pic/port unit logical-unit-number family mlfr-uni-nni]** hierarchy level:

```
[edit chassis fpc slot-number pic slot-number]
mlfr-uni-nni-bundles number;
```

```
[edit interfaces t1-fpc/pic/port unit logical-unit-number family mlfr-uni-nni]
bundle lsq-fpc/pic/port:channel;
```



**NOTE:** Link services IQ interfaces support both T1 and E1 physical interfaces. These instructions apply to T1 interfaces, but the configuration for E1 interfaces is similar.

To configure the link services IQ interface properties, include the following statements at the **[edit interfaces lsq- fpc/pic/port:channel]** hierarchy level:

```
[edit interfaces lsq- fpc/pic/port:channel]
encapsulation multilink-frame-relay-uni-nni;
dce;
mlfr-uni-nni-options {
  acknowledge-retries number;
  acknowledge-timer milliseconds;
  action-red-differential-delay (disable-tx | remove-link);
  drop-timeout milliseconds;
  fragment-threshold bytes;
  hello-timer milliseconds;
  link-layer-overhead percent;
  lmi-type (ansi | itu);
  minimum-links number;
  mrru bytes;
  n391 number;
  n392 number;
  n393 number;
  red-differential-delay milliseconds;
  t391 number;
  t392 number;
  yellow-differential-delay milliseconds;
}
unit logical-unit-number {
  dlci dlci-identifier;
  family inet {
    address address;
```

```
}
}
```

The link services IQ channel represents the FRF.16 bundle. Four queues are associated with each DLCI. A scheduler removes packets from the queues according to a scheduling policy. On the link services IQ interface, you typically designate one queue to have strict priority. The remaining queues are serviced in proportion to weights you configure.

For link services IQ interfaces, a strict-high-priority queue might starve the other three queues because traffic in a strict-high-priority queue is transmitted before any other queue is serviced. This implementation is unlike the standard Junos CoS implementation in which a strict-high-priority queue does round-robin with high-priority queues, as described in the *Junos OS Class of Service Library for Routing Devices*.

If the bundle has more than one link, you must include the **per-unit-scheduler** statement at the **[edit interfaces lsq-fpc/pic/port:channel]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port:channel]
  per-unit-scheduler;
```

For FRF.16, you can assign a single scheduler map to the link services IQ interface (**lsq**) and to each link services IQ DLCI, or you can assign different scheduler maps to the various DLCIs of the bundle, as shown in [“Example: Configuring an LSQ Interface as an NxT1 Bundle Using FRF.16” on page 658](#).

For the constituent links of an FRF.16 bundle, you do not need to configure a custom scheduler. Because LFI and multiclass are not supported for FRF.16, the traffic from each constituent link is transmitted from queue 0. This means you should allow most of the bandwidth to be used by queue 0. For M Series and T Series routers, the default schedulers' transmission rate and buffer size percentages for queues 0 through 3 are 95, 0, 0, and 5 percent. These default schedulers send all user traffic to queue 0 and all network-control traffic to queue 3, and therefore are well suited to the behavior of FRF.16. If desired, you can configure a custom scheduler that explicitly replicates the 95, 0, 0, and 5 percent queuing behavior, and apply it to the constituent links.



**NOTE:** For M320 and T Series routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

If the member link belonging to one MLPP, MLFR, or MFR bundle interface is moved to another bundle interface, or the links are swapped between two bundle interfaces, a commit is required between the delete and add operations to ensure that the configuration is applied correctly.

To configure and apply the scheduling policy, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
  interfaces {
    lsq-fpc/pic/port:channel {
      unit logical-unit-number {
```

```

        scheduler-map map-name;
    }
}
forwarding-classes {
    queue queue-number class-name;
}
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}
schedulers {
    scheduler-name {
        buffer-size (percent percentage | remainder | temporal microseconds);
        priority priority-level;
        transmit-rate (rate | percent percentage | remainder) <exact>;
    }
}

```

To configure packet fragmentation handling on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```

[edit class-of-service]
fragmentation-maps {
    map-name {
        forwarding-class class-name {
            fragment-threshold bytes;
        }
    }
}

```

For FRF.16 traffic, only multilink encapsulated (fragmented and sequenced) queues are supported. This is the default queuing behavior for all forwarding classes. FRF.16 does not allow for nonencapsulated traffic because the protocol requires that all packets carry the fragmentation header. If a large packet is split into multiple fragments, the fragments must have consecutive sequential numbers. Therefore, you cannot include the **no-fragmentation** statement at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level for FRF.16 traffic. For FRF.16, if you want to carry voice or any other latency-sensitive traffic, you should not use slow links. At T1 speeds and above, the serialization delay is small enough so that you do not need to use explicit LFI.

When a packet is removed from a multilink-encapsulated queue, the software gives the packet an FRF.16 header. The FRF.16 header contains a sequence number field, which is filled with the next available sequence number from a counter. The software then places the packet on one of the *N* different T1 links. The link is chosen on a packet-by-packet basis to balance the load across the various T1 links.

If the packet exceeds the minimum link MTU, or if a queue has a fragment threshold configured at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level, the software splits the packet into two or more fragments, which are assigned consecutive multilink sequence numbers. The outgoing link for each fragment is selected independently of all other fragments.

If you do not include the **fragment-threshold** statement in the fragmentation map, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number*]** or **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options]** hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest MTU of all the links in the bundle.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the maximum received reconstructed unit (MRRU) by including the **mrru** statement at the **[edit interfaces *lsq-fpc/port* unit *logical-unit-number*]** or **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options]** hierarchy level. The MRRU is similar to the MTU but is specific to link services interfaces. By default, the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see [“Configuring MRRU on Multilink and Link Services Logical Interfaces” on page 1391](#).

The *N* different T1 interfaces link to another router, which can be from Juniper Networks or another vendor. The router at the far end gathers packets from all the T1 links. Because each packet has an FRF.16 header, the sequence number field is used to put the packet back into sequence number order.

### Example: Configuring an LSQ Interface as an NxT1 Bundle Using FRF.16

Configure an NxT1 bundle using FRF.16 with multiple CoS scheduler maps:

```
[edit chassis fpc 1 pic 3]
adaptive-services {
  service-package layer-2;
}
mlfr-uni-nni-bundles 2; # Creates channelized LSQ interfaces/FRF.16 bundles.
[edit interfaces]
t1-0/0/0 {
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    family mlfr-uni-nni {
      bundle lsq-1/3/0:1;
    }
  }
}
t1-0/0/1 {
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    family mlfr-uni-nni {
      bundle lsq-1/3/0:1;
    }
  }
}
lsq-1/3/0:1 { # Bundle link consisting of t1-0/0/0 and t1-0/0/1
  per-unit-scheduler;
  encapsulation multilink-frame-relay-uni-nni;
  dce; # One end needs to be configured as DCE.
  mlfr-uni-nni-bundle-options {
    drop-timeout 180;
    fragment-threshold 64;
  }
}
```

```

hello-timer 180;
minimum-links 2;
mrru 3000;
link-layer-overhead 0.5;
}
unit 0 {
  dlci 26; # Each logical unit maps a single DLCI.
  family inet {
    address 10.2.3.4/24;
  }
}
unit 1 {
  dlci 42;
  family inet {
    address 10.20.30.40/24;
  }
}
unit 2 {
  dlci 69;
  family inet {
    address 10.20.30.40/24;
  }
}
[edit class-of-service]
scheduler-maps {
  sched-map-lsq0 {
    forwarding-class af scheduler af-scheduler-lsq0;
    forwarding-class be scheduler be-scheduler-lsq0;
    forwarding-class ef scheduler ef-scheduler-lsq0;
    forwarding-class nc scheduler nc-scheduler-lsq0;
  }
  sched-map-lsq1 {
    forwarding-class af scheduler af-scheduler-lsq1;
    forwarding-class be scheduler be-scheduler-lsq1;
    forwarding-class ef scheduler ef-scheduler-lsq1;
    forwarding-class nc scheduler nc-scheduler-lsq1;
  }
}
schedulers {
  af-scheduler-lsq0 {
    transmit-rate percent 60;
    buffer-size percent 60;
    priority low;
  }
  be-scheduler-lsq0 {
    transmit-rate percent 30;
    buffer-size percent 30;
    priority low;
  }
  ef-scheduler-lsq0 {
    transmit-rate percent 5;
    buffer-size percent 5;
    priority strict-high;
  }
  nc-scheduler-lsq0 {
    transmit-rate percent 5;

```

```
        buffer-size percent 5;
        priority high;
    }
    af-scheduler-lsq1 {
        transmit-rate percent 50;
        buffer-size percent 50;
        priority low;
    }
    be-scheduler-lsq1 {
        transmit-rate percent 30;
        buffer-size percent 30;
        priority low;
    }
    ef-scheduler-lsq1 {
        transmit-rate percent 15;
        buffer-size percent 15;
        priority strict-high;
    }
    nc-scheduler-lsq1 {
        transmit-rate percent 5;
        buffer-size percent 5;
        priority high;
    }
}
interfaces {
    lsq-1/3/0:1 { # MLFR FRF.16
        unit 0 {
            scheduler-map sched-map-lsq0;
        }
        unit 1 {
            scheduler-map sched-map-lsq1;
        }
    }
}
```

**Related Documentation**

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using MLPPP on page 649](#)
- [Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.15 on page 672](#)
- [Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP on page 673](#)
- [Link Services Configuration for Junos Interfaces](#)

---

## Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using MLPPP and LFI

---

When you configure a single fractional T1 interface, it is called a logical interface, because it can represent, for example, a routing adjacency.

The logical link services IQ interface represents the MLPPP bundle. Four queues are associated with the logical interface. A scheduler removes packets from the queues according to a scheduling policy. Typically, you designate one queue to have strict priority, and the remaining queues are serviced in proportion to weights you configure.

To configure a single fractional T1 interface using MLPPP and LFI, you associate one DS0 (fractional T1) interface with a link services IQ interface. To associate a fractional T1 interface with a link services IQ interface, include the **bundle** statement at the **[edit interfaces ds-fpc/pic/port:channel unit logical-unit-number family mlppp]** hierarchy level:

```
[edit interfaces ds-fpc/pic/port:channel unit logical-unit-number family mlppp]
bundle lsq-fpc/pic/port.logical-unit-number;
```



**NOTE:** Link services IQ interfaces support both T1 and E1 physical interfaces. These instructions apply to T1 interfaces, but the configuration for E1 interfaces is similar.

To configure the link services IQ interface properties, include the following statements at the **[edit interfaces lsq-fpc/pic/port unit logical-unit-number]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port unit logical-unit-number]
drop-timeout milliseconds;
encapsulation multilink-ppp;
fragment-threshold bytes;
link-layer-overhead percent;
minimum-links number;
mrru bytes;
short-sequence;
family inet {
    address address;
}
```

For MLPPP, assign a single scheduler map to the link services IQ (**lsq**) interface and to each constituent link. The default schedulers for M Series and T Series routers, which assign 95, 0, 0, and 5 percent bandwidth for the transmission rate and buffer size of queues 0, 1, 2, and 3, are not adequate when you configure LFI or multiclass traffic. Therefore, for MLPPP, you should configure a single scheduler with nonzero percent transmission rates and buffer sizes for queues 0 through 3, and assign this scheduler to the link services IQ (**lsq**) interface and to each constituent link and to each constituent link, as shown in [“Example: Configuring an LSQ Interface for a Fractional T1 Interface Using MLPPP and LFI”](#) on page 663.



**NOTE:** For M320 and T Series routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

To configure and apply the scheduling policy, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
interfaces {
    ds-fpc/pic/port:channel {
        scheduler-map map-name;
    }
}
```

```

forwarding-classes {
    queue queue-number class-name;
}
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}
schedulers {
    scheduler-name {
        buffer-size (percent percentage | remainder | temporal microseconds);
        priority priority-level;
        transmit-rate (rate | percent percentage | remainder) <exact>;
    }
}

```

For link services IQ interfaces, a strict-high-priority queue might starve all the other queues because traffic in a strict-high priority queue is transmitted before any other queue is serviced. This implementation is unlike the standard Junos CoS implementation in which a strict-high-priority queue receives infinite credits and does round-robin with high-priority queues, as described in the *Junos OS Class of Service Library for Routing Devices*.

After the scheduler removes a packet from a queue, a certain action is taken. The action depends on whether the packet came from a multilink encapsulated queue (fragmented and sequenced) or a nonencapsulated queue (hashed with no fragmentation). Each queue can be designated as either multilink encapsulated or nonencapsulated, independently of the other. By default, traffic in all forwarding classes is multilink encapsulated. To configure packet fragmentation handling on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```

[edit class-of-service]
fragmentation-maps {
    map-name {
        forwarding-class class-name {
            fragment-threshold bytes;
            no-fragmentation;
        }
    }
}

```

If you require the queue to transmit small packets with low latency, configure the queue to be nonencapsulated by including the **no-fragmentation** statement. If you require the queue to transmit large packets with normal latency, configure the queue to be multilink encapsulated by including the **fragment-threshold** statement. If you require the queue to transmit large packets with low latency, we recommend using a faster link and configuring the queue to be nonencapsulated. For more information about fragmentation maps, see [“Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces” on page 633](#).

When a packet is removed from a multilink-encapsulated queue, it is fragmented. If the packet exceeds the minimum link MTU, or if a queue has a fragment threshold configured at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level, the software splits the packet into two or more fragments, which are assigned consecutive multilink sequence numbers.

If you do not include the **fragment-threshold** statement in the fragmentation map, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest MTU of all the links in the bundle.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the maximum received reconstructed unit (MRRU) by including the **mrru** statement at the **[edit interfaces *lsq-fpc/port* unit *logical-unit-number*]** hierarchy level. The MRRU is similar to the MTU, but is specific to link services interfaces. By default the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see [“Configuring MRRU on Multilink and Link Services Logical Interfaces” on page 1391](#).

When a packet is removed from a multilink-encapsulated queue, the software gives the packet an MLPPP header. The MLPPP header contains a sequence number field, which is filled with the next available sequence number from a counter. The software then places the packet on the fractional T1 link. Traffic from another queue might be interleaved between two fragments of the packet.

When a packet is removed from a nonencapsulated queue, it is transmitted with a plain PPP header. The packet is then placed on the fractional T1 link as soon as possible. If necessary, the packet is placed between the fragments of a packet from another queue.

The fractional T1 interface links to another router, which can be from Juniper Networks or another vendor. The router at the far end gathers packets from the fractional T1 link. If a packet has an MLPPP header, the software assumes the packet is a fragment of a larger packet, and the fragment number field is used to reassemble the larger packet. If the packet has a plain PPP header, the software accepts the packet in the order in which it arrives, and the software makes no attempt to reassemble or reorder the packet.

### Example: Configuring an LSQ Interface for a Fractional T1 Interface Using MLPPP and LFI

Configure a single fractional T1 logical interface:

```
[edit interfaces]
lsq-0/2/0 {
  per-unit-scheduler;
  unit 0 {
    encapsulation multilink-ppp;
    link-layer-overhead 0.5;
    family inet {
      address 10.40.1.1/30;
    }
  }
}
ct3-1/0/0 {
  partition 1 interface-type ct1;
}
ct1-1/0/0:1 {
  partition 1 timeslots 1-2 interface-type ds;
}
ds-1/0/0:1:1 {
```

```
encapsulation ppp;
unit 0 {
    family mlppp {
        bundle lsq-0/2/0.0;
    }
}
[edit class-of-service]
interfaces {
    ds-1/0/0:1:1 { # multilink PPP constituent link
        unit 0 {
            scheduler-map sched-map1;
        }
    }
}
forwarding-classes {
    queue 0 be;
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
}
scheduler-maps {
    sched-map1 {
        forwarding-class af scheduler af-scheduler;
        forwarding-class be scheduler be-scheduler;
        forwarding-class ef scheduler ef-scheduler;
        forwarding-class nc scheduler nc-scheduler;
    }
}
schedulers {
    af-scheduler {
        transmit-rate percent 20;
        buffer-size percent 20;
        priority low;
    }
    be-scheduler {
        transmit-rate percent 20;
        buffer-size percent 20;
        priority low;
    }
    ef-scheduler {
        transmit-rate percent 50;
        buffer-size percent 50;
        priority strict-high; # voice queue
    }
    nc-scheduler {
        transmit-rate percent 10;
        buffer-size percent 10;
        priority high;
    }
}
fragmentation-maps {
    fragmap-1 {
        forwarding-class be {
            fragment-threshold 180;
        }
        forwarding-class ef {
```

```

        fragment-threshold 100;
    }
}
[edit interfaces]
lsq-0/2/0 {
    unit 0 {
        fragmentation-map fragmap-1;
    }
}

```

**Related  
Documentation**

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12 on page 665](#)
- [Link Services Configuration for Junos Interfaces](#)

## Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12

To configure a single fractional T1 interface using FRF.16, you associate a DS0 interface with a link services IQ (lsq) interface. When you configure a single fractional T1, the fractional T1 carries a potentially large number of Frame Relay PVCs identified by their DLCIs. Each DLCI is called a logical interface, because it can represent, for example, a routing adjacency. To associate the DS0 interface with a link services IQ interface, include the **bundle** statement at the **[edit interfaces ds-fpc/pic/port:channel unit logical-unit-number family mlfr-end-to-end]** hierarchy level:

```

[edit interfaces ds-fpc/pic/port:channel unit logical-unit-number family mlfr-end-to-end]
bundle lsq-fpc/pic/port.logical-unit-number;

```



**NOTE:** Link services IQ interfaces support both T1 and E1 physical interfaces. These instructions apply to T1 interfaces, but the configuration for E1 interfaces is similar.

To configure the link services IQ interface properties, include the following statements at the **[edit interfaces lsq-fpc/pic/port unit logical-unit-number]** hierarchy level:

```

[edit interfaces lsq-fpc/pic/port unit logical-unit-number]
drop-timeout milliseconds;
encapsulation multilink-frame-relay-end-to-end;
fragment-threshold bytes;
link-layer-overhead percent;
minimum-links number;
mrru bytes;
short-sequence;
family inet {
    address address;
}

```

The logical link services IQ interface represents the FRF.12 bundle. Four queues are associated with each logical interface. A scheduler removes packets from the queues

according to a scheduling policy. Typically, you designate one queue to have strict priority, and the remaining queues are serviced in proportion to weights you configure.

For FRF.12, assign a single scheduler map to the link services IQ interface (**lsq**) and to each constituent link. For M Series and T Series routers, the default schedulers, which assign 95, 0, 0, and 5 percent bandwidth for the transmission rate and buffer size of queues 0, 1, 2, and 3, are not adequate when you configure LFI or multiclass traffic. Therefore, for FRF.12, you should configure schedulers with nonzero percent transmission rates and buffer sizes for queues 0 through 3, and assign them to the link services IQ interface (**lsq**) and to each constituent link, as shown in [“Examples: Configuring an LSQ Interface for a Fractional T1 Interface Using FRF.12” on page 668](#).



**NOTE:** For M320 and T Series routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

To configure and apply the scheduling policy, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
interfaces {
  ds-fpc/pic/port.channel {
    scheduler-map map-name;
  }
}
forwarding-classes {
  queue queue-number class-name;
}
scheduler-maps {
  map-name {
    forwarding-class class-name scheduler scheduler-name;
  }
}
schedulers {
  scheduler-name {
    buffer-size (percent percentage | remainder | temporal microseconds);
    priority priority-level;
    transmit-rate (rate | percent percentage | remainder) <exact>;
  }
}
```

For link services IQ interfaces, a strict-high-priority queue might starve the other three queues because traffic in a strict-high-priority queue is transmitted before any other queue is serviced. This implementation is unlike the standard Junos CoS implementation in which a strict-high-priority queue does round-robin with high-priority queues, as described in the *Junos OS Class of Service Library for Routing Devices*.

After the scheduler removes a packet from a queue, a certain action is taken. The action depends on whether the packet came from a multilink encapsulated queue (fragmented and sequenced) or a nonencapsulated queue (hashed with no fragmentation). Each queue can be designated as either multilink encapsulated or nonencapsulated,

independently of the other. By default, traffic in all forwarding classes is multilink encapsulated. To configure packet fragmentation handling on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
fragmentation-maps {
  map-name {
    forwarding-class class-name {
      fragment-threshold bytes;
      no-fragmentation;
    }
  }
}
```

If you require the queue to transmit small packets with low latency, configure the queue to be nonencapsulated by including the **no-fragmentation** statement. If you require the queue to transmit large packets with normal latency, configure the queue to be multilink encapsulated by including the **fragment-threshold** statement. If you require the queue to transmit large packets with low latency, we recommend using a faster link and configuring the queue to be nonencapsulated. For more information about fragmentation maps, see [“Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces” on page 633](#).

When a packet is removed from a multilink-encapsulated queue, it is fragmented. If the packet exceeds the minimum link MTU, or if a queue has a fragment threshold configured at the **[edit class-of-service fragmentation-maps map-name forwarding-class class-name]** hierarchy level, the software splits the packet into two or more fragments, which are assigned consecutive multilink sequence numbers.

If you do not include the **fragment-threshold** statement in the fragmentation map, the fragmentation threshold you set at the **[edit interfaces interface-name unit logical-unit-number]** hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest MTU of all the links in the bundle.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the maximum received reconstructed unit (MRRU) by including the **mrru** statement at the **[edit interfaces lsq-fpc/pic/port unit logical-unit-number]** hierarchy level. The MRRU is similar to the MTU but is specific to link services interfaces. By default, the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see [“Configuring MRRU on Multilink and Link Services Logical Interfaces” on page 1391](#).

When a packet is removed from a multilink-encapsulated queue, the software gives the packet an FRF.12 header. The FRF.12 header contains a sequence number field, which is filled with the next available sequence number from a counter. The software then places the packet on the fractional T1 link. Traffic from another queue might be interleaved between two fragments of the packet.

When a packet is removed from a nonencapsulated queue, it is transmitted with a plain Frame Relay header. The packet is then placed on the fractional T1 link as soon as possible. If necessary, the packet is placed between the fragments of a packet from another queue.

The fractional T1 interface links to another router, which can be from Juniper Networks or another vendor. The router at the far end gathers packets from the fractional T1 link. If a packet has an FRF.12 header, the software assumes the packet is a fragment of a larger packet, and the fragment number field is used to reassemble the larger packet. If the packet has a plain Frame Relay header, the software accepts the packet in the order in which it arrives, and the software makes no attempt to reassemble or reorder the packet.

A whole packet from a nonencapsulated queue can be placed between fragments of a multilink-encapsulated queue. However, fragments from one multilink-encapsulated queue cannot be interleaved with fragments from another multilink-encapsulated queue. This is the intent of the specification FRF.12, *Frame Relay Fragmentation Implementation Agreement*. If fragments from two different queues were interleaved, the header fields might not have enough information to separate the fragments.

### Examples: Configuring an LSQ Interface for a Fractional T1 Interface Using FRF.12

#### FRF.12 with Fragmentation and Without LFI

This example shows a 128 KB DS0 interface. There is one traffic stream on **ge-0/0/0**, which is classified into queue 0 (**be**). Packets are fragmented in the link services IQ (**lsq-**) interface according to the threshold configured in the fragmentation map.

```
[edit chassis]
fpc 0 {
  pic 3 {
    adaptive-services {
      service-package layer-2;
    }
  }
}
[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family inet {
      address 20.1.1.1/24 {
        arp 20.1.1.2 mac 00.90.1b.12.34.56;
      }
    }
  }
}
cel-0/2/0 {
  partition 1 timeslots 1-2 interface-type ds;
}
ds-0/2/0:1 {
  no-keepalives;
  dce;
  encapsulation frame-relay;
  unit 0 {
    dlci 100;
    family mlfr-end-to-end {
      bundle lsq-0/3/0.0;
    }
  }
}
```

```

    }
  }
  lsq-0/3/0 {
    per-unit-scheduler;
    unit 0 {
      encapsulation multilink-frame-relay-end-to-end;
      family inet {
        address 10.200.0.78/30;
      }
    }
  }
  fxp0 {
    unit 0 {
      family inet {
        address 172.16.1.162/24;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.1/32;
      }
    }
  }
  [edit class-of-service]
  forwarding-classes {
    queue 0 be;
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
  }
  interfaces {
    lsq-0/3/0 {
      unit 0 {
        fragmentation-map map1;
      }
    }
  }
  fragmentation-maps {
    map1 {
      forwarding-class {
        be {
          fragment-threshold 160;
        }
      }
    }
  }
}

```

#### FRF.12 with Fragmentation and LFI

This example shows a 512 KB DS0 bundle and four traffic streams on **ge-0/0/0** that are classified into four queues. The fragment size is 160 for queue 0, queue 1, and queue 2. The voice stream on queue 3 has LFI configured.

```
[edit chassis]
fpc 0 {
  pic 3 {
    adaptive-services {
      service-package layer-2;
    }
  }
}
[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family inet {
      address 20.1.1.1/24 {
        arp 20.1.1.2 mac 00:90:1b:12:34:56;
      }
    }
  }
}
cel-0/2/0 {
  partition 1 timeslots 1-8 interface-type ds;
}
ds-0/2/0:1 {
  no-keepalives;
  dce;
  encapsulation frame-relay;
  unit 0 {
    dlci 100;
    family mlfr-end-to-end {
      bundle lsq-0/3/0.0;
    }
  }
}
lsq-0/3/0 {
  per-unit-scheduler;
  unit 0 {
    encapsulation multilink-frame-relay-end-to-end;
    family inet {
      address 10.200.0.78/30;
    }
  }
}
[edit class-of-service]
classifiers {
  inet-precedence ge-interface-classifier {
    forwarding-class be {
      loss-priority low code-points 000;
    }
    forwarding-class ef {
      loss-priority low code-points 010;
    }
    forwarding-class af {
      loss-priority low code-points 100;
    }
    forwarding-class nc {
      loss-priority low code-points 110;
    }
  }
}
```

```

}
forwarding-classes {
    queue 0 be;
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
}
interfaces {
    lsq-0/3/0 {
        unit 0 {
            scheduler-map sched2;
            fragmentation-map map2;
        }
    }
    ds-0/2/0:1 {
        scheduler-map link-map2;
    }
    ge-0/0/0 {
        unit 0 {
            classifiers {
                inet-precedence ge-interface-classifier;
            }
        }
    }
}
scheduler-maps {
    sched2 {
        forwarding-class be scheduler economy;
        forwarding-class ef scheduler business;
        forwarding-class af scheduler stream;
        forwarding-class nc scheduler voice;
    }
    link-map2 {
        forwarding-class be scheduler link-economy;
        forwarding-class ef scheduler link-business;
        forwarding-class af scheduler link-stream;
        forwarding-class nc scheduler link-voice;
    }
}
fragmentation-maps {
    map2 {
        forwarding-class {
            be {
                fragment-threshold 160;
            }
            ef {
                fragment-threshold 160;
            }
            af {
                fragment-threshold 160;
            }
            nc {
                no-fragmentation;
            }
        }
    }
}

```

```
schedulers {
  economy {
    transmit-rate percent 26;
    buffer-size percent 26;
  }
  business {
    transmit-rate percent 26;
    buffer-size percent 26;
  }
  stream {
    transmit-rate percent 35;
    buffer-size percent 35;
  }
  voice {
    transmit-rate percent 13;
    buffer-size percent 13;
  }
  link-economy {
    transmit-rate percent 26;
    buffer-size percent 26;
  }
  link-business {
    transmit-rate percent 26;
    buffer-size percent 26;
  }
  link-stream {
    transmit-rate percent 35;
    buffer-size percent 35;
  }
  link-voice {
    transmit-rate percent 13;
    buffer-size percent 13;
  }
}
}
```

**Related  
Documentation**

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using MLPPP and LFI on page 660](#)
- *Link Services Configuration for Junos Interfaces*

---

## Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.15

This example configures an *N*xT1 bundle using FRF.15 on a link services IQ interface. FRF.15 is similar to FRF.12, as described in “[Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12” on page 665](#). The difference is that FRF.15 supports multiple physical links in a bundle, whereas FRF.12 supports only one physical link per bundle. For the Junos OS implementation of FRF.15, you can configure one DLCI per physical link.



**NOTE:** Link services IQ interfaces support both T1 and E1 physical interfaces. This example refers to T1 interfaces, but the configuration for E1 interfaces is similar.

```
[edit interfaces]
lsq-1/3/0 {
  per-unit-scheduler;
  unit 0 {
    encapsulation multilink-frame-relay-end-to-end;
  }
}
unit 1 {
  encapsulation multilink-frame-relay-end-to-end;
}
# First physical link
t1-1/1/0:1 {
  encapsulation frame-relay;
  unit 0 {
    dlci 69;
    family mlfr-end-to-end {
      bundle lsq-1/3/0.0;
    }
  }
}
# Second physical link
t1-1/1/0:2 {
  encapsulation frame-relay;
  unit 0 {
    dlci 13;
    family mlfr-end-to-end {
      bundle lsq-1/3/0.0;
    }
  }
}
```

**Related  
Documentation**

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using MLPPP on page 649](#)
- [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using FRF.16 on page 655](#)
- [Link Services Configuration for Junos Interfaces](#)

## Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP

This example bundles a single T3 interface on a link services IQ interface with MLPPP encapsulation. Binding a single T3 interface to a multilink bundle allows you to configure compressed RTP (CRTP) on the T3 interface.

This scenario applies to MLPPP bundles only. The Junos OS does not currently support CRTP over Frame Relay. For more information, see [“Configuring Services Interfaces for Voice Services” on page 696](#).

There is no need to configure LFI at DS3 speeds, because the packet serialization delay is negligible.

```
[edit interfaces]
t3-0/0/0 {
  unit 0 {
    family mlppp {
      bundle lsq-1/3/0.1;
    }
  }
}
lsq-1/3/0.1 {
  encapsulation multilink-ppp;
}
compression {
  rtp {
    # cRTP parameters go here
    #
    port minimum 2000 maximum 64009;
  }
}
```

This configuration uses a default fragmentation map, which results in all forwarding classes (queues) being sent out with a multilink header.

To eliminate multilink headers, you can configure a fragmentation map in which all queues have the **no-fragmentation** statement at the **[edit class-of-service fragmentation-maps map-name forwarding-class class-name]** hierarchy level, and attach the fragmentation map to the **lsq-1/3/0.1** interface, as shown here:

```
[edit class-of-service]
fragmentation-maps {
  fragmap {
    forwarding-class {
      be {
        no-fragmentation;
      }
      af {
        no-fragmentation;
      }
      ef {
        no-fragmentation;
      }
      nc {
        no-fragmentation;
      }
    }
  }
}
interfaces {
  lsq-1/3/0.1 {
    fragmentation-map fragmap;
  }
}
```

- Related Documentation**
- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
  - [Configuring LSQ Interfaces as NxT1 or NxEl Bundles Using MLPPP on page 649](#)
  - [Configuring LSQ Interfaces for Single Fractional T1 or El Interfaces Using MLPPP and LFI on page 660](#)
  - [Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP on page 677](#)
  - [Link Services Configuration for Junos Interfaces](#)

## Configuring LSQ Interfaces as T3 or OC3 Bundles Using FRF.12

This example configures a clear-channel T3 or OC3 interface with multiple logical interfaces (DLCIs) on the link. In this scenario, each DLCI represents a customer. DLCIs are shaped at the egress PIC to a particular speed (*NxDSO*). This allows you to configure LFI using FRF.12 End-to-End Protocol on Frame Relay DLCIs.

To do this, first configure logical interfaces (DLCIs) on the physical interface. Then bundle the DLCIs, so that there is only one DLCI per bundle.

The physical interface must be capable of per-DLCI scheduling, which allows you to attach shaping rates to each DLCI. For more information, see the *Junos OS Network Interfaces Library for Routing Devices*.

To prevent fragment drops at the egress PIC, you must assign a shaping rate to the link services IQ logical interfaces and to the egress DLCIs. Shaping rates on DLCIs specify how much bandwidth is available for each DLCI. The shaping rate on link services IQ interfaces should match the shaping rate assigned to the DLCI that is associated with the bundle.

Egress interfaces also must have a scheduler map attached. The queue that carries voice should be strict-high-priority, while all other queues should be low-priority. This makes LFI possible.

This example shows voice traffic in the **ef** queue. The voice traffic is interleaved with bulk data. Alternatively, you can use multiclass MLPPP to carry multiple classes of traffic in different multilink classes, as described in [“Configuring Multiclass MLPPP on LSQ Interfaces” on page 636](#).

```
[edit interfaces]
t3-0/0/0 {
  per-unit-scheduler;
  encapsulation frame-relay;
  unit 0 {
    dlc1 69;
    family mlfr-end-to-end {
      bundle lsq-1/3/0.0;
    }
  }
  unit 1 {
    dlc1 42;
    family mlfr-end-to-end {
```

```

        bundle lsq-1/3/0.1;
    }
}
lsq-1/3/0 {
    unit 0 {
        encapsulation multilink-frame-relay-end-to-end;
    }
    fragment-threshold 320; # Multilink packets must be fragmented
}
unit 1 {
    encapsulation multilink-frame-relay-end-to-end;
}
fragment-threshold 160;
[edit class-of-service]
scheduler-maps {
    sched { # Scheduling parameters that apply to bundles on AS or Multiservices PICs.
        ...
    }
    pic-sched {
        # Scheduling parameters for egress DLCIs.
        # The voice queue should be strict-high priority.
        # All other queues should be low priority.
        ...
    }
}
fragmentation-maps {
    fragmap {
        forwarding-class {
            ef {
                no-fragmentation;
            }
            # Voice is carried in the ef queue.
            # It is interleaved with bulk data.
        }
    }
}
interfaces {
    t3-0/0/0 {
        unit 0 {
            shaping-rate 512k;
            scheduler-map pic-sched;
        }
        unit 1 {
            shaping-rate 128k;
            scheduler-map pic-sched;
        }
    }
}
lsq-1/3/0 { # Assign fragmentation and scheduling to LSQ interfaces.
    unit 0 {
        shaping-rate 512k;
        scheduler-map sched;
        fragmentation-map fragmap;
    }
    unit 1 {
        shaping-rate 128k;
        scheduler-map sched;
    }
}

```

```

        fragmentation-map fragmap;
    }
}

```

For more information about how FRF.12 works with links services IQ interfaces, see [“Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12” on page 665.](#)

#### Related Documentation

- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
- [Link Services Configuration for Junos Interfaces](#)
- [Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP on page 673](#)

## Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP

This example configures an ATM2 IQ interface with MLPPP bundled with link services IQ interfaces. This allows you to configure LFI on ATM virtual circuits.

For this type of configuration, the ATM2 IQ interface must have LLC encapsulation.

The following ATM PICs are supported in this scenario:

- 2-port OC-3/STM1 ATM2 IQ
- 4-port DS3 ATM2 IQ

Virtual circuit multiplexed PPP over AAL5 is not supported. Frame Relay is not supported. Bundling of multiple ATM VCs into a single logical interface is not supported.

Unlike DS3 and OC3 interfaces, there is no need to create a separate scheduler map for the ATM PIC. For ATM, you define CoS components at the **[edit interfaces at-fpc/pic/port atm-options]** hierarchy level, as described in the *Junos OS Network Interfaces Library for Routing Devices*.



**NOTE:** Do not configure RED profiles on ATM logical interfaces that are bundled. Drops do not occur at the ATM interface.

In this example, two ATM VCs are configured and bundled into two link services IQ bundles. A fragmentation map is used to interleave voice traffic with other multilink traffic. Because MLPPP is used, each link services IQ bundle can be configured for CRTP.

```

[edit interfaces]
at-1/2/0 {
  atm-options {
    vpi 0;
    pic-type atm2;
  }
  unit 0 {
    vci 0.69;
    encapsulation atm-mlppp-llc;
  }
}

```

```

        family mlppp {
            bundle lsq-1/3/0.10;
        }
    }
    unit 1 {
        vci 0.42;
        encapsulation atm-mlppp-llc;
        family mlppp {
            bundle lsq-1/3/0.11;
        }
    }
}
lsq-1/3/0 {
    unit 10 {
        encapsulation multilink-ppp;
    }
    # Large packets must be fragmented.
    # You can specify fragmentation for each forwarding class.
    fragment-threshold 320;
    compression {
        rtp {
            port minimum 2000 maximum 64009;
        }
    }
}
unit 11 {
    encapsulation multilink-ppp;
}
fragment-threshold 160;
[edit class-of-service]
scheduler-maps {
    sched { # Scheduling parameters that apply to LSQ bundles on AS or Multiservices PICs.
        ...
    }
}
fragmentation-maps {
    fragmap {
        forwarding-class {
            ef {
                no-fragmentation;
            }
        }
    }
}
}
interfaces { # Assign fragmentation and scheduling parameters to LSQ interfaces.
lsq-1/3/0 {
    unit 0 {
        shaping-rate 512k;
        scheduler-map sched;
        fragmentation-map fragmap;
    }
    unit 1 {
        shaping-rate 128k;
        scheduler-map sched;
        fragmentation-map fragmap;
    }
}
}

```

- Related Documentation**
- [Layer 2 Service Package Capabilities and Interfaces on page 616](#)
  - *Link Services Configuration for Junos Interfaces*



## CHAPTER 24

# Summary of Link Services IQ Configuration Statements

The following sections explain each of the Link Services Intelligent Queuing (IQ) statements. The statements are organized alphabetically.

### cisco-interoperability

---

<b>Syntax</b>	<code>cisco-interoperability send-lip-remove-link-for-link-reject;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	FRF.16 interoperability settings.
<b>Options</b>	<b>send-lip-remove-link-for-link-reject</b> —Send Link Integrity Protocol remove link when an add-link rejection message is received.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring SONET APS Interoperability with Cisco Systems FRF.16 on page 619</a></li></ul>

## forwarding-class

---

<b>Syntax</b>	<pre>forwarding-class <i>class-name</i> {     (<i>fragment-threshold bytes</i>   <i>no-fragmentation</i>);     <i>multilink-class number</i>; }</pre>
<b>Hierarchy Level</b>	[edit class-of-service <a href="#">fragmentation-maps</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For link services IQ (<b>lsq</b>) interfaces only, define a forwarding class name and associated fragmentation properties within a fragmentation map.</p> <p>The <b>fragment-threshold</b> and <b>no-fragmentation</b> statements are mutually exclusive.</p>
<b>Default</b>	If you do not include this statement, the traffic in forwarding class <b><i>class-name</i></b> is fragmented.
<b>Options</b>	<p><b><i>class-name</i></b>—Name of the forwarding class.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces on page 633</a></li></ul>

## fragment-threshold

<b>Syntax</b>	<code>fragment-threshold <i>bytes</i>;</code>
<b>Hierarchy Level</b>	<code>[edit class-of-service fragmentation-maps <a href="#">forwarding-class</a> <i>class-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services IQ ( <b>lsq</b> ) interfaces only, set the fragmentation threshold for an individual forwarding class.
<b>Default</b>	If you do not include this statement, the fragmentation threshold you set at the <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code> or <code>[edit interfaces <i>interface-name</i> mlfr-uni-nni-bundle-options]</code> hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest maximum transmission unit (MTU) of all the links in the bundle.
<b>Options</b>	<p><b><i>bytes</i></b>—Maximum size, in bytes, for multilink packet fragments. Any nonzero value must be a multiple of 64 bytes.</p> <p><b>Range:</b> 128 through 16,320 bytes</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces on page 633</a></li> </ul>

## fragmentation-map

<b>Syntax</b>	<code>fragmentation-map <i>map-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services IQ ( <b>lsq</b> ) interfaces only, associate a fragmentation map with a multilink PPP interface or MLFR FRF.16 DLCI.
<b>Default</b>	If you do not include this statement, traffic in all forwarding classes is fragmented.
<b>Options</b>	<b><i>map-name</i></b> —Name of the fragmentation map.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces on page 633</a></li> </ul>

## fragmentation-maps

---

<b>Syntax</b>	<pre>fragmentation-maps {   map-name {     forwarding-class class-name {       (fragment-threshold bytes   no-fragmentation);       multilink-class number;     }   } }</pre>
<b>Hierarchy Level</b>	[edit class-of-service]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services IQ (lsq) interfaces only, define fragmentation properties for individual forwarding classes.
<b>Default</b>	If you do not include this statement, traffic in all forwarding classes is fragmented.
<b>Options</b>	<p><i>map-name</i>—Name of the fragmentation map.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces on page 633</a></li></ul>

## hot-standby

<b>Syntax</b>	hot-standby;
<b>Hierarchy Level</b>	[edit interfaces <i>rlsnumber</i> <b>redundancy-options</b> ], [edit interfaces <i>rlsnumber:number</i> <b>redundancy-options</b> ] [edit interfaces <i>rspnumber</i> <b>redundancy-options</b> ] [edit interfaces <i>rmsnumber</i> <b>redundancy-options</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	For one-to-one AS, rsp, or rms redundancy configurations, specify that the failure detection and recovery must take place in less than 5 seconds. For FRF.15 (MLFR) and FRF.16 (MFR) configuration, specify the switch over time of 5 seconds and less for FRF.15 and a maximum of 10 seconds for FRF.16.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621</a></li> <li>• <a href="#">Configuring AS or Multiservices PIC Redundancy on page 806</a></li> </ul>

## link-layer-overhead

<b>Syntax</b>	link-layer-overhead <i>percent</i> ;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> mlfr-uni-nni-bundle-options], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services IQ (lsq) interfaces only, configure the percentage of total bundle bandwidth to be set aside for link-layer overhead. Link-layer overhead accounts for the bit stuffing on serial links. Bit stuffing is used to prevent data from being interpreted as control information. Overhead resulting from link-layer encapsulation and framing is computed automatically.
<b>Options</b>	<p><b>percent</b>—Percentage of total bundle bandwidth to be set aside for link-layer overhead.</p> <p><b>Range:</b> 0 through 50 percent</p> <p><b>Default:</b> 0 percent</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring CoS Scheduling Queues on Logical LSQ Interfaces on page 630</a></li> </ul>

## lsq-failure-options

---

<b>Syntax</b>	<code>lsq-failure-options {     no-termination-request;     trigger-link-failure <i>interface-name</i>; }</code>
<b>Hierarchy Level</b>	[edit interfaces <i>lsq-fpc/pic/port</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	For link services IQ ( <b>lsq</b> ) interfaces only, define the failure recovery option settings.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Association between LSQ and SONET Interfaces on page 618</a></li></ul>

## multilink-class

---

<b>Syntax</b>	<code>multilink-class <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit class-of-service fragmentation-maps <i>map-name</i> forwarding-class <i>class-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services IQ ( <b>lsq</b> ) interfaces only, map a forwarding class into a multiclass MLPPP (MCML).  The <b>multilink-class</b> statement and <b>no-fragmentation</b> statements are mutually exclusive.
<b>Options</b>	<i>number</i> —The multilink class assigned to this forwarding class. <b>Range:</b> 0 through 7 <b>Default:</b> None
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces on page 633</a></li><li>• <a href="#">Configuring Multiclass MLPPP on LSQ Interfaces on page 636</a></li><li>• <a href="#">Configuring Fragmentation by Forwarding Class</a></li><li>• <a href="#">Junos OS Services Interfaces Library for Routing Devices</a></li><li>• <a href="#">multilink-max-classes on page 687</a></li></ul>

## multilink-max-classes

---

<b>Syntax</b>	<code>multilink-max-classes <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services IQ (lsq) interfaces only, configure the number of multilink classes to be negotiated when a link joins the bundle.
<b>Options</b>	<b><i>number</i></b> —The number of multilink classes to be negotiated when a link joins the bundle. <b>Range:</b> 1 through 8 <b>Default:</b> None
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Multiclass MLPPP on LSQ Interfaces on page 636</a></li></ul>

## no-fragmentation

---

<b>Syntax</b>	no-fragmentation;
<b>Hierarchy Level</b>	[edit class-of-service fragmentation-maps <b>forwarding-class</b> <i>class-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For link services IQ (<b>lsq</b>) interfaces only, set traffic on a particular forwarding class to be interleaved, rather than fragmented. This statement specifies that no extra fragmentation header is prepended to the packets received on this queue and that static-link load balancing is used to ensure in-order packet delivery.</p> <p>Static-link load balancing is done based on packet payload. For IP version 4 (IPv4) and IP version 6 (IPv6) traffic, the link is chosen based on a hash computed from the source address, destination address, and protocol. If the IP payload is Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) traffic, the hash also includes source port and destination port. For MPLS traffic, the hash includes all MPLS labels and fields in the payload, whether the MPLS payload is IPv4 or IPv6.</p>
<b>Default</b>	If you do not include this statement, the traffic in forwarding class <i>class-name</i> is fragmented.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces on page 633</a></li></ul>

## no-per-unit-scheduler

---

<b>Syntax</b>	no-per-unit-scheduler;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 11.4.
<b>Description</b>	To enable traffic control profiles to be applied at FRF.16 bundle (physical) interface level, disable the per-unit scheduler, which is enabled by default. This statement and the <b>shared-scheduler</b> statement are mutually exclusive.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Oversubscribing Interface Bandwidth</a></li></ul>

## no-termination-request

---

<b>Syntax</b>	no-termination-request;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ppp-options], [edit interfaces lsq-fpc/pic/port <i>lsq-failure-options</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4. Support at the [edit interfaces <i>interface-name</i> ppp-options] hierarchy level added in Junos OS Release 8.3.
<b>Description</b>	Inhibit PPP termination-request messages to the remote host if the primary circuit fails.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Association between LSQ and SONET Interfaces on page 618</a></li></ul>

## per-unit-scheduler

<b>Syntax</b>	<code>per-unit-scheduler;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 13.2 on 16x10GE MPC and MPC3E line cards. Statement introduced in Junos OS Release 13.2 on PTX Series Packet Transport Routers. Statement introduced in Junos OS Release 13.3 on MPC4E line cards.
<b>Description</b>	For Channelized OC3 IQ, Channelized OC12 IQ, Channelized STM1 IQ, Channelized T3 IQ, Channelized E1 IQ, E3 IQ, link services IQ interfaces (lsq-), link services (ls-) on J Series routers, Gigabit Ethernet IQ, Gigabit Ethernet IQ2 and IQ2-E, and 10-, 40-, and 100-Gigabit Ethernet interfaces (including the 16x10GE MPC), enable the association of scheduler map names with logical interfaces.



**NOTE:** Per-unit scheduling is not supported on T1 interfaces configured on the Channelized OC12 IQ PIC.



**NOTE:** On Gigabit Ethernet IQ2 and IQ2-E PICs without the `per-unit-scheduler` statement, the entire PIC supports 4071 VLANs and the user can configure all the VLANs on the same port.

On Gigabit Ethernet IQ2 and IQ2-E PICs with the `per-unit-scheduler` statement, the entire PIC supports  $1024 - 2 * \text{number of ports}$  (1024 minus two times the number of ports), because each port is allocated two default schedulers.

When including the `per-unit-scheduler` statement, you must also include the `vlan-tagging` statement or the `flexible-vlan-tagging` statement (to apply scheduling to VLANs) or the `encapsulation frame-relay` statement (to apply scheduling to DLCIs) at the [edit interfaces *interface-name*] hierarchy level.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Applying Scheduler Maps and Shaping Rate to DLCIs and VLANs</i></li> <li>• <i>vlan-tagging</i></li> <li>• <i>flexible-vlan-tagging</i></li> <li>• <i>Applying Scheduling and Shaping to VLANs</i></li> <li>• <i>Configuring Virtual LAN Queuing and Shaping on PTX Series Packet Transport Routers</i></li> </ul>

## preserve-interface

---

<b>Syntax</b>	<code>preserve-interface;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> sonet-options aps]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	<p>Provide link PIC replication, providing MLPPP link redundancy at the port level. This feature is supported with SONET APS and the following link PICs:</p> <ul style="list-style-type: none"><li>• Channelized OC3 IQ PIC</li><li>• Channelized OC12 IQ PIC</li><li>• Channelized STM1 IQ PIC</li></ul> <p>Link PIC replication provides the ability to add two sets of links, one from the active SONET PIC and the other from the standby SONET PIC, to the same bundle. If the active SONET PIC fails, links from the standby PIC are used without triggering link renegotiation. All the negotiated state is replicated from the active links to the standby links to prevent link renegotiation.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Link State Replication for Redundant Link PICs on page 624</a></li></ul>

## primary

---

<b>Syntax</b>	<code>primary interface-name;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>rlsqnumber</i> <a href="#">redundancy-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	Specify the primary Link Services IQ PIC interface.
<b>Options</b>	<i>interface-name</i> —The identifier for the Link Services IQ PIC interface, which must be of the form <i>lsq-fpc/pic/port</i> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621</a></li></ul>

## redundancy-options

---

<b>Syntax</b>	<pre>redundancy-options {   (hot-standby   warm-standby);   primary lsq-fpc/pic/port;   secondary lsq-fpc/pic/port; }</pre>
<b>Hierarchy Level</b>	[edit interfaces rlsqnumber]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	Specify the primary and secondary (backup) Link Services IQ PIC interfaces.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621</a></li></ul>

## secondary

---

<b>Syntax</b>	<pre>secondary interface-name;</pre>
<b>Hierarchy Level</b>	[edit interfaces rlsqnumber <b>redundancy-options</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	Specify the secondary (backup) Link Services IQ PIC interface.
<b>Options</b>	<b>interface-name</b> —The identifier for the Link Services IQ PIC interface, which must be of the form <b>lsq-fpc/pic/port</b> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621</a></li></ul>

## trigger-link-failure

---

<b>Syntax</b>	<code>trigger-link-failure <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>lsq-fpc/pic/port</i> <a href="#">lsq-failure-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	List of SONET interfaces connected to the LSQ interface that can implement Automatic Protection Switching (APS) if the Link Services IQ PIC fails.
<b>Options</b>	<i>interface-name</i> —Name of SONET interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Association between LSQ and SONET Interfaces on page 618</a></li></ul>

## warm-standby

---

<b>Syntax</b>	<code>warm-standby;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>rlsqnumber</i> <a href="#">redundancy-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.0.
<b>Description</b>	For AS or Multiservices PIC redundancy configurations, specify that the failure detection and recovery involves one backup PIC supporting multiple working PICs. Recovery time is not guaranteed.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621</a></li></ul>



# Voice Services Configuration Guidelines

The Adaptive Services (AS) and Multiservices PICs support the compressed Real-Time Transport Protocol (C RTP) on the **lsq-fpc/pic/port** interface type. This enables voice over IP (VoIP) traffic to use low-speed links more effectively, by compressing the 40-byte IP/User Datagram Protocol (UDP)/RTP header down to from 2 to 4 bytes in most cases.



**NOTE:** J Series routers also support VoIP routing through the Avaya TGM550 media gateway module. This is a separate product from the adaptive services suite and is not supported on M Series and T Series routers. For more information, see the *Junos OS Feature Support Reference for SRX Series and J Series Devices*.

For link services IQ interfaces (**lsq**) only, you can configure C RTP with multiclass MLPPP (MCML). MCML greatly simplifies packet ordering issues that occur when multiple links are used. Without MCML, all voice traffic belonging to a single flow is hashed to a single link in order to avoid packet ordering issues. With MCML, you can assign voice traffic to a high-priority class, and you can use multiple links. For more information about MCML support on link services IQ interfaces, see [“Configuring Link Services and CoS on Services PICs” on page 646](#).

Link services IQ interfaces use a bundle configuration. For more information, see [“Layer 2 Service Package Capabilities and Interfaces” on page 616](#) and [“Multilink and Link Services Logical Interface Configuration Overview” on page 1385](#).



**NOTE:** On LSQ interfaces, all multilink traffic for a single bundle is sent to a single processor. If C RTP is enabled on the bundle, it adds overhead to the CPU. Because T3 network interfaces support only one link per bundle, make sure you configure a fragmentation map for compressed traffic on these interfaces and specify the no-fragmentation option. For more information, see [“Configuring Delay-Sensitive Packet Interleaving” on page 698](#) and [“Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces” on page 633](#).

Voice services do not require a separate service rules configuration, but you need to configure both services interfaces and network interfaces, as described in the following topics:

- [Configuring Services Interfaces for Voice Services on page 696](#)
- [Configuring Encapsulation for Voice Services on page 699](#)
- [Configuring Network Interfaces for Voice Services on page 700](#)
- [Examples: Configuring Voice Services on page 701](#)

## Configuring Services Interfaces for Voice Services

---

You define voice service properties such as compression by configuring statements and values for a voice services interface, specified by the interface type **lsq**-. You can include the following statements:

```
encapsulation mlppp;  
family inet {  
    address address;  
}  
compression {  
    rtp {  
        f-max-period number;  
        maximum-contexts number <force>;  
        port {  
            minimum port-number;  
            maximum port-number;  
        }  
        queues [ queue-numbers ];  
    }  
}  
fragment-threshold bytes;
```

You can include these statements at the following hierarchy levels:

- **[edit interfaces (lsq | ls)-fpc/pic/port unit logical-unit-number]**
- **[edit logical-systems logical-system-name interfaces (lsq | ls)-fpc/pic/port unit logical-unit-number]**

The following sections provide detailed instructions for configuring for voice services on services interfaces:

- [Configuring the Logical Interface Address for the MLPPP Bundle on page 696](#)
- [Configuring Compression of Voice Traffic on page 697](#)
- [Configuring Delay-Sensitive Packet Interleaving on page 698](#)
- [Example: Configuring Compression of Voice Traffic on page 698](#)

### Configuring the Logical Interface Address for the MLPPP Bundle

To configure the logical address for the MLPPP bundle, include the **address** statement:

```
address address {
```

```
...
}
```

You can configure this statement at the following hierarchy levels:

- [edit interfaces (lsq | ls)-fpc/pic/port unit logical-unit-number family inet]
- [edit logical-systems logical-system-name interfaces (lsq | ls)-fpc/pic/port unit logical-unit-number family inet]

**address** specifies an IP address for the interface. AS and Multiservices PICs support only IP version 4 (IPv4) addresses, which are therefore configured under the **family inet** statement.

For information on other addressing properties you can configure that are not specific to service interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

## Configuring Compression of Voice Traffic

You can specify how a services interface handles voice traffic compression by including the **compression** statement:

```
compression {
  rtp {
    f-max-period number;
    maximum-contexts number <force>;
    port {
      minimum port-number;
      maximum port-number;
    }
    queues [ queue-numbers ];
  }
}
```

You can include this statement at the following hierarchy levels:

- [edit interfaces (lsq | ls)-fpc/pic/port unit logical-unit-number]
- [edit logical-systems logical-system-name interfaces (lsq | ls)-fpc/pic/port unit logical-unit-number]

The following statements configure the indicated compression properties:

- **f-max-period number**—Sets the maximum number of compressed packets to insert between the transmission of full headers. If you do not include the statement, the default is 255 packets.
- **maximum-contexts number <force>**—Specifies the maximum number of RTP contexts to accept during negotiation. The optional **force** statement requires the PIC to use the value specified for maximum RTP contexts, regardless of the negotiated value. This option enables interoperation with Junos OS Releases that base the RTP context value on link speed.
- **port, minimum port-number, and maximum port-number**—Specify the lower and upper boundaries for a range of UDP destination port values on which RTP compression takes

effect. Values for **port-number** can range from 0 through 65,535. RTP compression is applied to traffic transiting the ports within the specified range.

- **queues [ queue-numbers ]**—Specifies one or more of queues **q0**, **q1**, **q2**, and **q3**. RTP compression is applied to the traffic in the specified queues.



**NOTE:** If you specify both a port range and one or more queues, compression takes place if either condition is met.

## Configuring Delay-Sensitive Packet Interleaving

When you configure CRTP, the software automatically enables link fragmentation and interleaving (LFI). LFI reduces excessive delays by fragmenting long packets into smaller packets and interleaving them with real-time frames. This allows real-time and non-real-time data frames to be carried together on lower-speed links without causing excessive delays to the real-time traffic. When the peer interface receives the smaller fragments, it reassembles the fragments into their original packet. For example, short delay-sensitive packets, such as packetized voice, can race ahead of larger delay-insensitive packets, such as common data packets.

By default, LFI is always active when you include the **compression rtp** statement at the **[edit interfaces interface-name unit logical-unit-number]** hierarchy level. You control the operation of LFI indirectly by setting the **fragment-threshold** statement on the same logical interface. For example, if you include the **fragment-threshold 256** statement at the **[edit interfaces interface-name unit logical-unit-number]** hierarchy level, all IP packets larger than 256 bytes are fragmented.

## Example: Configuring Compression of Voice Traffic

Configure compression on a T1 interface with MLPPP encapsulation. Configure fragmentation for all IP packets larger than 128 bytes.

```
[edit interfaces]
t1-1/0/0 {
  unit 0 {
    family mlppp {
      bundle lsq-1/1/0.1;
    }
  }
}
lsq-1/1/0 {
  encapsulation mlppp;
  unit 1 {
    compression {
      rtp {
        port minimum 2000 maximum 64009;
      }
    }
  }
  family inet {
    address 30.1.1.2/24;
  }
}
```

```

        fragment-threshold 128;
    }
}

```

#### Related Documentation

- [Voice Services Overview on page 79](#)
- [Configuring Encapsulation for Voice Services on page 699](#)
- [Configuring Network Interfaces for Voice Services on page 700](#)
- [Examples: Configuring Voice Services on page 701](#)

## Configuring Encapsulation for Voice Services

Voice services interfaces support the following logical interface encapsulation types:

- Multilink Point-to-Point Protocol (MLPPP), which is the default encapsulation
- ATM2 IQ MLPPP over AAL5 LLC
- Frame Relay PPP

For general information on encapsulation, see the *Junos OS Network Interfaces Library for Routing Devices*. You can also configure physical interface encapsulation on voice services interfaces.

To configure voice services encapsulation, include the **encapsulation** statement:

```
encapsulation type;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

For voice services interfaces, the valid values for the **type** variable are **atm-mlppp-llc**, **frame-relay-ppp** or **multilink-ppp**.

You must also configure the physical interface with the corresponding encapsulation type, either Frame Relay or PPP. LSQ interfaces are supported by the following physical interface types: ATM2 IQ, DS3, E1, E3, OC3, OC12, STM1, and T1, including the channelized versions of these interfaces. For examples, see [“Examples: Configuring Voice Services” on page 701](#).



**NOTE:** The only protocol type supported with **frame-relay-ppp** encapsulation is **family mlppp**.

#### Related Documentation

- [Voice Services Overview on page 79](#)
- [Configuring Services Interfaces for Voice Services on page 696](#)
- [Configuring Network Interfaces for Voice Services on page 700](#)

- [Examples: Configuring Voice Services on page 701](#)

## Configuring Network Interfaces for Voice Services

---

To complete a voice services interface configuration, you need to configure the physical network interface with either MLPPP encapsulation and a voice services bundle or PPP encapsulation and a compression interface, as described in the following sections:

- [Configuring Voice Services Bundles with MLPPP Encapsulation on page 700](#)
- [Configuring the Compression Interface with PPP Encapsulation on page 700](#)

### Configuring Voice Services Bundles with MLPPP Encapsulation

For voice services interfaces, you configure the link bundle as a channel. The physical interface is usually connected to networks capable of supporting MLPPP; the interface types supported for voice traffic are T1, E1, T3, E3, OC3, OC12, and STM1, including channelized versions of these interfaces.



---

#### NOTE:

For M Series routers and T Series routers, the following caveats apply:

- Maximum supported throughput on the bundle interfaces is 45 Mbps.
  - Bundling of the logical interfaces under a T3 physical interface into the same or different bundles is not supported.
- 

To configure a physical interface link for MLPPP, include the following statement:

**bundle** *interface-name*;

You can configure this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family mlppp]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family mlppp]

When you configure **family mlppp**, no other protocol configuration is allowed. For more information on link bundles, see “[Configuring the Links in a Multilink or Link Services Bundle](#)” on page 1383.

### Configuring the Compression Interface with PPP Encapsulation

To configure the physical interface for PPP encapsulation, you also need to specify the services interface to be used for voice compression: a Link Services IQ (**lsq-**) interface.

To configure the compression interface, include the **compression-device** statement:

**compression-device** *interface-name*;

You can configure this statement at the following hierarchy levels:

- `[edit interfaces (lsq | ls)-fpc/pic/port unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces (lsq | ls)-fpc/pic/port unit logical-unit-number]`

**Related  
Documentation**

- [Voice Services Overview on page 79](#)
- [Configuring Services Interfaces for Voice Services on page 696](#)
- [Configuring Encapsulation for Voice Services on page 699](#)
- [Examples: Configuring Voice Services on page 701](#)

## Examples: Configuring Voice Services

Configure voice services using a T1 physical interface and MLPPP bundle encapsulation:

```
[edit interfaces]
t1-0/2/0:1 {
  encapsulation ppp;
  unit 0 {
    family mlppp {
      bundle lsq-1/3/0.1;
    }
  }
}
lsq-1/3/0 {
  unit 1 {
    encapsulation mlppp;
    family inet {
      address 10.5.5.2/30;
    }
    compression {
      rtp {
        f-max-period 100;
        queues [ q1 q2 ];
        port {
          minimum 16384;
          maximum 32767;
        }
      }
    }
    fragment-threshold 128;
  }
}
```

Configure voice services using Frame Relay encapsulation without bundling:

```
[edit interfaces]
t1-1/0/0 {
  encapsulation frame-relay;
  unit 0 {
    dlci 100;
    encapsulation frame-relay-ppp;
    compression-device lsq-2/0/0.0;
  }
}
```

```
}
lsq-2/0/0 {
  unit 0 {
    compression {
      rtp {
        f-max-period 100;
        queues [ q1 q2 ];
        port {
          minimum 16000;
          maximum 32000;
        }
      }
    }
  }
  family inet {
    address 10.1.1.1/32;
  }
}
}
```

Configure voice services using an ATM2 physical interface (the corresponding class-of-service configuration is provided for illustration):

```
[edit interfaces]
at-1/2/0 {
  atm-options {
    vpi 0;
    pic-type atm2; # only ATM2 PICs are supported
  }
  unit 0 {
    vci 0.69;
    encapsulation atm-mlppp-llc;
    family mlppp {
      bundle lsq-1/3/0.10;
    }
  }
  unit 1 {
    vci 0.42;
    encapsulation atm-mlppp-llc;
    family mlppp {
      bundle lsq-1/3/0.11;
    }
  }
}
lsq-1/3/0 {
  unit 10 {
    encapsulation multilink-ppp;
  }
  # Large packets need to be fragmented.
  # Fragmentation can also be specified per forwarding class.
  fragment-threshold 320;
  compression {
    rtp {
      port minimum 2000 maximum 64009;
    }
  }
}
```

```

unit 11 {
    encapsulation multilink-ppp;
}
fragment-threshold 160;
[edit class-of-service]
scheduler-maps {
    sched {
        # Scheduling parameters apply to bundles on the AS or Multiservices PIC.
        # Unlike DS3/SONET interfaces, there is no need to create
        # a separate scheduler map for the ATM PIC. ATM defines
        # CoS constructs under the [edit interfaces at-fpc/pic/port] hierarchy.
        ...
    }
}
fragmentation-maps {
    fragmap {
        forwarding-class {
            ef {
                # In this example, voice is carried in the ef queue.
                # It is interleaved with bulk data.
                # Alternatively, you could use multiclass MLPPP to
                # carry multiple classes of traffic in different
                # multilink classes.
                no-fragmentation;
            }
        }
    }
}
}
interfaces {
    # Assign fragmentation and scheduling parameters to LSQ interfaces.
    lsq-1/3/0 {
        unit 0 {
            shaping-rate 512k;
            scheduler-map sched;
            fragmentation-map fragmap;
        }
        unit 1 {
            shaping-rate 128k;
            scheduler-map sched;
            fragmentation-map fragmap;
        }
    }
}
}

```

**Related  
Documentation**

- [Voice Services Overview on page 79](#)
- [Configuring Services Interfaces for Voice Services on page 696](#)
- [Configuring Encapsulation for Voice Services on page 699](#)
- [Configuring Network Interfaces for Voice Services on page 700](#)



## CHAPTER 26

# Summary of Voice Services Configuration Statements

The following sections explain each of the voice services statements. The statements are organized alphabetically.

- [address \(Interfaces\) on page 706](#)
- [bundle on page 706](#)
- [compression on page 707](#)
- [compression-device \(Interfaces\) on page 707](#)
- [encapsulation on page 708](#)
- [f-max-period on page 708](#)
- [family \(Interfaces\) on page 709](#)
- [fragment-threshold \(Interfaces LSQ\) on page 710](#)
- [interfaces on page 710](#)
- [maximum-contexts on page 711](#)
- [port on page 712](#)
- [queues on page 712](#)
- [rtp on page 713](#)
- [unit \(Interfaces\) on page 714](#)

## address (Interfaces)

---

<b>Syntax</b>	<code>address address {     ... }</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> <i>family</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> <i>family</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the interface address.
<b>Options</b>	<b>address</b> —Address of the interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li><li>• <a href="#">Configuring the Logical Interface Address for the MLPPP Bundle on page 696</a></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## bundle

---

<b>Syntax</b>	<code>bundle (lsq-<i>fpc/pic/port</i>   ... );</code>
<b>Hierarchy Level</b>	[edit interfaces lsq- <i>fpc/pic/port</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> mlppp]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Associate the voice services interface with the logical interface it is joining.
<b>Options</b>	<b>lsq-<i>fpc/pic/port</i></b> —Name of the voice services interface you are linking.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Voice Services Bundles with MLPPP Encapsulation on page 700</a></li></ul>

## compression

<b>Syntax</b>	<pre> compression {   rtp {     f-max-period <i>number</i>;     maximum-contexts <i>number</i> &lt;force&gt;;     port {       minimum <i>port-number</i>;       maximum <i>port-number</i>;     }     queues [ <i>queue-numbers</i> ];   } } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the compression properties for voice services traffic.  The remaining statements are described separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Compression of Voice Traffic on page 697</a></li> </ul>

## compression-device (Interfaces)

<b>Syntax</b>	compression-device <i>interface-name</i> ;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit (Interfaces)</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.5.
<b>Description</b>	Specify the compression interface for voice services traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Compression Interface with PPP Encapsulation on page 700</a></li> </ul>

## encapsulation

---

<b>Syntax</b>	<code>encapsulation type;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the logical link-layer encapsulation type.
<b>Options</b>	<b>atm-mlppp-llc</b> —For ATM2 IQ physical interfaces only, use Multilink Point-to-Point Protocol (MLPPP) over AAL5 LLC encapsulation.  <b>frame-relay-ppp</b> —For Frame Relay circuits, use Frame Relay PPP encapsulation.  <b>multilink-ppp</b> —By default, voice services logical interfaces use MLPPP encapsulation.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Encapsulation for Voice Services on page 699</a></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## f-max-period

---

<b>Syntax</b>	<code>f-max-period number;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>compression</b> <i>rtp</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>compression</b> <i>rtp</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the maximum number of compressed packets allowed between the transmission of full headers in a compressed Real-time Transport Protocol (RTP) traffic stream.
<b>Options</b>	<b>number</b> —Maximum number of packets. <b>Default:</b> 256
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Compression of Voice Traffic on page 697</a></li></ul>

## family (Interfaces)

<b>Syntax</b>	<pre>family (inet   mlppp   ...) {     address address {         ...     }     bundle interface-name; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure protocol family information for the logical interface.
<b>Options</b>	<p><i>family</i>—Protocol family:</p> <ul style="list-style-type: none"> <li>• <b>inet</b>—IP version 4</li> <li>• <b>mlppp</b>—MLPPP</li> </ul> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li> <li>• <a href="#">Configuring Network Interfaces for Voice Services on page 700</a></li> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li> </ul>

## fragment-threshold (Interfaces LSQ)

---

<b>Syntax</b>	<code>fragment-threshold bytes;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>lsq-fpc/pic/port unit logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>lsq-fpc/pic/port unit logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For voice services interfaces, set the fragmentation threshold, in bytes.
<b>Options</b>	<b>bytes</b> —Maximum size, in bytes, for multilink packet fragments. The value must be a multiple of 64 bytes, because zero is also a multiple of 64 bytes. <b>Range:</b> 128 through 16,320 bytes <b>Default:</b> 0 bytes (no fragmentation)
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Delay-Sensitive Packet Interleaving on page 698</a></li></ul>

## interfaces

---

<b>Syntax</b>	<code>interfaces { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure interfaces on the router.
<b>Default</b>	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## maximum-contexts

---

<b>Syntax</b>	<code>maximum-contexts <i>number</i> &lt;force&gt;;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">unit</a> <i>logical-unit-number</i> <a href="#">compression rtp</a> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <a href="#">unit</a> <i>logical-unit-number</i> <a href="#">compression rtp</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.5.
<b>Description</b>	Specify the maximum number of RTP contexts to accept during negotiation.
<b>Options</b>	<p><i>number</i>—Maximum number of contexts.</p> <p><i>force</i>—(Optional) Requires the PIC to use the value specified for maximum RTP contexts, regardless of the negotiated value. This option allows the software to interoperate with Junos OS Releases that base the RTP context value on link speed.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Compression of Voice Traffic on page 697</a></li> </ul>

## port

---

<b>Syntax</b>	<pre>port {     minimum <i>port-number</i>;     maximum <i>port-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>lsq-fpc/pic/port</i> <b>unit</b> <i>logical-unit-number</i> <b>compression</b> <i>rtp</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>lsq-fpc/pic/port</i> <b>unit</b> <i>logical-unit-number</i> <b>compression</b> <i>rtp</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For voice services interfaces only, specify a range of User Datagram Protocol (UDP) destination port numbers in which RTP compression takes place.
<b>Options</b>	<b>minimum <i>port-number</i></b> —Specify the minimum port number. <b>Range:</b> 0 through 65,535  <b>maximum <i>port-number</i></b> —Specify the maximum port number. <b>Range:</b> 0 through 65,535
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Compression of Voice Traffic on page 697</a></li></ul>

## queues

---

<b>Syntax</b>	<pre>queues [ <i>queue-numbers</i> ];</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>compression</b> <i>rtp</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>compression</b> <i>rtp</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For voice services interfaces only, assign queue numbers on which RTP compression takes place.
<b>Options</b>	<b>queues <i>queue-numbers</i></b> —Assign one or more of the following queues: <b>q0</b> , <b>q1</b> , <b>q2</b> , and <b>q3</b> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Compression of Voice Traffic on page 697</a></li></ul>

## rtp

---

<b>Syntax</b>	<pre> rtp {     f-max-period <i>number</i>;     maximum-contexts <i>number</i> &lt;force&gt;;     port {         minimum <i>port-number</i>;         maximum <i>port-number</i>;     }     queues [ <i>queue-numbers</i> ]; } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>compression</b> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>compression</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Configure the RTP properties for voice services traffic.</p> <p>The remaining statements are described separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Compression of Voice Traffic on page 697</a></li> </ul>

## unit (Interfaces)

---

**Syntax**    `unit logical-unit-number {  
              compression {  
                rtp {  
                  f-max-period number;  
                  maximum-contexts number <force>;  
                port {  
                  minimum port-number;  
                  maximum port-number;  
                }  
              queues [ queue-numbers ];  
            }  
          }  
          compression-device interface-name;  
          encapsulation type;  
          family family {  
            address address {  
              ...  
            }  
            bundle (lsq-fpc/pic/port | ...);  
          }  
          }  
          }`

**Hierarchy Level**    [edit [interfaces](#) interface-name ]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

**Options**    *logical-unit-number*—Number of the logical unit.

**Range:** 0 through 16,384

The remaining statements are explained separately.

**Required Privilege**    interface—To view this statement in the configuration.

**Level**    interface-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Network Interfaces Library for Routing Devices* for other statements that do not affect services interfaces.
- [Configuring Services Interfaces for Voice Services on page 696](#)
- *Junos OS Network Interfaces Library for Routing Devices*

# Class-of-Service Configuration Guidelines

To configure class of service (CoS) features on Adaptive Services (AS) and Multiservices PICs, include the **cos** statement at the **[edit services]** hierarchy level:

```
cos {
  application-profile profile-name {
    ftp {
      data {
        dscp (alias | bits);
        forwarding-class class-name;
      }
    }
    sip {
      video {
        dscp (alias | bits);
        forwarding-class class-name;
      }
      voice {
        dscp (alias | bits);
        forwarding-class class-name;
      }
    }
  }
}
rule rule-name {
  match-direction (input | output | input-output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address (CoS) address;
      destination-prefix-list list-name <except>;
      source-address address;
      source-prefix-list list-name <except>;
    }
    then {
      application-profile profile-name;
      dscp (alias | bits);
      forwarding-class class-name;
      syslog;
      (reflexive | reverse) {
        application-profile profile-name;
        dscp (alias | bits);
        forwarding-class class-name;
      }
    }
  }
}
```

```
        syslog;  
    }  
}  
}  
}  
rule-set rule-set-name {  
    [ rule rule-names ];  
}  
}
```



**NOTE:** CoS behavior aggregate (BA) classification is not supported on services interfaces.

---

This chapter contains the following sections:

- [Restrictions and Cautions for CoS Configuration on Services Interfaces on page 716](#)
- [Configuring CoS Rules on page 717](#)
- [Configuring CoS Rule Sets on page 722](#)
- [Examples: Configuring CoS on Services Interfaces on page 722](#)

---

## Restrictions and Cautions for CoS Configuration on Services Interfaces

---

The following restrictions and cautions apply to CoS configuration on services interfaces:

- The adaptive services interface does not support scheduling, only DiffServ marking and queue assignment. You must configure scheduling at the **[edit class-of-service]** hierarchy level on the output interface or fabric.
- In the default configuration, queues 1 and 2 receive 0 percent bandwidth. If packets will be assigned to these queues, you must configure a scheduling map.
- You must issue a **commit full** command before using custom forwarding-class names in the configuration.
- Only the Junos standard DiffServ names can be used in the configuration. Custom names are not recognized.
- On M Series routers, you can configure rewrite rules that change packet headers and attach the rules to output interfaces. These rules might overwrite the DSCP marking configured on an AS or MultiServices PIC. It is important to keep this adverse effect in mind and use care when creating system-wide configurations.

For example, knowing that the AS or MultiServices PIC can mark packets with any ToS or DSCP value and the output interface is restricted to only eight DSCP values, rewrite rules on the output interface condense the mapping from 64 to 8 values with overall loss of granularity. In this case, you have the following options:

- Remove the rewrite rules from the output interface.
- Configure the output interface to include the most important mappings.

- Related Documentation**
- [Class of Service Overview on page 82](#)
  - [Configuring CoS Rules on page 717](#)
  - [Configuring CoS Rule Sets on page 722](#)
  - [Examples: Configuring CoS on Services Interfaces on page 722](#)

## Configuring CoS Rules

To configure a CoS rule, include the **rule** *rule-name* statement at the **[edit services cos]** hierarchy level:

```
[edit services cos]
rule rule-name {
  match-direction (input | output | input-output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address (CoS) address;
      destination-prefix-list list-name <except>;
      source-address address;
      source-prefix-list list-name <except>;
    }
    then {
      application-profile profile-name;
      dscp (alias | bits);
      forwarding-class class-name;
      syslog;
      (reflexive | reverse) {
        application-profile profile-name;
        dscp (alias | bits);
        forwarding-class class-name;
        syslog;
      }
    }
  }
}
```

Each CoS rule consists of a set of terms, similar to a filter configured at the **[edit firewall]** hierarchy level. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software.

The following sections explain how to configure the components of CoS rules:

- [Configuring Match Direction for CoS Rules on page 718](#)
- [Configuring Match Conditions In CoS Rules on page 718](#)

- [Configuring Actions in CoS Rules on page 719](#)
- [Example: Configuring CoS Rules on page 721](#)

## Configuring Match Direction for CoS Rules

Each rule must include a **match-direction** statement that specifies the direction in which the rule match is applied. To configure where the match is applied, include the **match-direction** statement at the **[edit services cos rule *rule-name*]** hierarchy level:

```
match-direction (input | output | input-output);
```

If you configure **match-direction input-output**, bidirectional rule creation is allowed.

The match direction is used with respect to the traffic flow through the AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.

With a next-hop service set, packet direction is determined by the interface used to route the packet to the AS or Multiservices PIC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the AS or Multiservices PIC, the packet direction is output. For more information on inside and outside interfaces, see [“Configuring Service Sets to be Applied to Services Interfaces” on page 742](#).

On the AS or Multiservices PIC, a flow lookup is performed. If no flow is found, rule processing is performed. All rules in the service set are considered. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that matches the packet direction are considered.

## Configuring Match Conditions In CoS Rules

To configure CoS match conditions, include the **from** statement at the **[edit services cos rule *rule-name* term *term-name*]** hierarchy level:

```
from {  
  application-sets set-name;  
  applications [ application-names ];  
  destination-address (CoS) address;  
  destination-prefix-list list-name <except>;  
  source-address address;  
  source-prefix-list list-name <except>;  
}
```

The source address and destination address can be either IPv4 or IPv6. You can use either the source address or the destination address as a match condition, in the same way that you would configure a firewall filter; for more information, see the *Routing Policy Feature Guide for Routing Devices*.

Alternatively, you can specify a list of source or destination prefixes by configuring the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either the **destination-prefix-list** or **source-prefix-list** statement in the CoS rule. For an example, see [“Examples: Configuring Stateful Firewall Rules” on page 392](#).

If you omit the **from** term, the router accepts all traffic and the default protocol handlers take effect:

- User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP) create a bidirectional flow with a predicted reverse flow.
- IP creates a unidirectional flow.

You can also include application protocol definitions you have configured at the **[edit applications]** hierarchy level; for more information, see [“Configuring Application Protocol Properties” on page 146](#).

- To apply one or more specific application protocol definitions, include the **applications** statement at the **[edit services cos rule rule-name term term-name from]** hierarchy level.
- To apply one or more sets of application protocol definitions you have defined, include the **application-sets** statement at the **[edit services cos rule rule-name term term-name from]** hierarchy level.



**NOTE:** If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the **[edit applications]** hierarchy level; you cannot specify these properties as match conditions.

## Configuring Actions in CoS Rules

To configure CoS actions, include the **then** statement at the **[edit services cos rule rule-name term term-name]** hierarchy level:

```
[edit services cos rule rule-name term term-name]
then {
  application-profile profile-name;
  dscp (alias | bits);
  forwarding-class class-name;
  syslog;
  (reflexive | reverse) {
    application-profile profile-name;
    dscp (alias | bits);
    forwarding-class class-name;
    syslog;
  }
}
```

The principal CoS actions are as follows:

- **dscp**—Causes the packet to be marked with the specified DiffServ code point (DSCP) value or alias.
- **forwarding-class**—Causes the packet to be assigned to the specified forwarding class.

For detailed information about DSCP values and forwarding classes, see “[Examples: Configuring CoS on Services Interfaces](#)” on page 722 or the *Junos OS Class of Service Library for Routing Devices*.

You can optionally set the configuration to record information in the system logging facility by including the **syslog** statement at the **[edit services cos rule rule-name term term-name then]** hierarchy level. This statement overrides any **syslog** setting included in the service set or interface default configuration.

For information about some additional CoS actions, see the following sections:

- [Configuring Application Profiles for Use as CoS Rule Actions on page 720](#)
- [Configuring Reflexive and Reverse CoS Rule Actions on page 721](#)

### Configuring Application Profiles for Use as CoS Rule Actions

You can optionally define one or more application profiles for inclusion in CoS actions. To configure application profiles, include the **application-profile** statement at the **[edit services cos]** hierarchy level:

```
[edit services cos]
application-profile profile-name {
  ftp {
    data {
      dscp (alias | bits);
      forwarding-class class-name;
    }
  }
  sip {
    video {
      dscp (alias | bits);
      forwarding-class class-name;
    }
    voice {
      dscp (alias | bits);
      forwarding-class class-name;
    }
  }
}
```

The **application-profile** statement includes two main components and three traffic types: **ftp** with the **data** traffic type and **sip** with the **video** and **voice** traffic types. You can set the appropriate **dscp** and **forwarding-class** values for each component within the application profile.



**NOTE:** The **ftp** and **sip** statements are not supported on Juniper Network MX Series 3D Universal Edge Routers.

You can apply the application profile to a CoS configuration by including it at the **[edit services cos rule rule-name term term-name then]** hierarchy level.

### Configuring Reflexive and Reverse CoS Rule Actions

CoS services are unidirectional. It might be necessary to specify different treatments for flows in opposite directions.

Regardless of whether a packet matches the input, output or input-output direction, flows in both directions are created. A forward, reverse, or forward-and-reverse CoS action is associated with each flow. Bear in mind that the flow in the opposite direction might end up having a CoS action associated with it that you have not specifically configured.

To control the direction in which service is applied, as distinct from the direction in which the rule match is applied, you can configure the (**reflexive** | **reverse**) statement at the **[edit services cos rule rule-name term term-name then]** hierarchy level:

```
[edit services cos rule rule-name term term-name then]
(reflexive | reverse) {
  application-profile profile-name;
  dscp (alias | bits);
  forwarding-class class-name;
  syslog;
}
```

The two actions are mutually exclusive:

- **reflexive** causes the equivalent opposing CoS action to be applied to flows in the opposite direction.
- **reverse** allows you to define the CoS behavior for flows in the reverse direction.

If you omit the statement, data flows inherit the CoS behavior of the forward control flow.

### Example: Configuring CoS Rules

The following example show a CoS configuration containing two rules, one for input matching on a specified application set and the other for output matching on a specified source address:

```
[edit services]
cos {
  rule my-cos-rule {
    match-direction input-output;
    term term1 {
      from {
        source-address 10.1.3.2/32;
        applications sip;
      }
      then {
        dscp ef;
        syslog;
      }
    }
    term term2 {
      from {
```

```
        destination-address 10.2.3.2;
        applications http;
    }
    then {
        dscp af21;
    }
}
}
```

**Related  
Documentation**

- [Class of Service Overview on page 82](#)
- [Restrictions and Cautions for CoS Configuration on Services Interfaces on page 716](#)
- [Configuring CoS Rule Sets on page 722](#)
- [Examples: Configuring CoS on Services Interfaces on page 722](#)

---

## Configuring CoS Rule Sets

The **rule-set** statement defines a collection of CoS rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then you specify the order of the rules by including the **rule-set** statement at the **[edit services cos]** hierarchy level with a **rule** statement for each rule:

```
rule-set rule-set-name {
    rule rule-name;
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing continues to the next rule in the rule set. If none of the rules matches the packet, the packet is dropped by default.

**Related  
Documentation**

- [Class of Service Overview on page 82](#)
- [Restrictions and Cautions for CoS Configuration on Services Interfaces on page 716](#)
- [Configuring CoS Rules on page 717](#)
- [Examples: Configuring CoS on Services Interfaces on page 722](#)

---

## Examples: Configuring CoS on Services Interfaces

To make settings consistent across Juniper Networks routers, you configure many CoS settings at the **[edit class-of-service]** hierarchy level to be used on services interfaces. When you commit this configuration along with what you configure at the **[edit services cos]** hierarchy level, these properties are applied to the AS or MultiServices PIC.

The following configuration examples at the **[edit class-of-service]** hierarchy level can be applied on services interfaces. For more information, see the *Junos OS Class of Service Library for Routing Devices*.



**NOTE:** The first two configurations, mapping forwarding-class name to forwarding-class ID and mapping forwarding-class name to queue number, are mutually exclusive.

<b>Mapping Forwarding-Class Name to Forwarding-Class ID</b>	<p>Map forwarding-class names to forwarding-class IDs:</p> <pre>[edit class-of-service] forwarding-classes {   forwarding-class fc0 0;   forwarding-class fc1 0;   forwarding-class fc2 1;   forwarding-class fc3 1;   forwarding-class fc4 2;   forwarding-class fc5 2;   forwarding-class fc6 3;   forwarding-class fc7 3;   forwarding-class fc8 4;   forwarding-class fc9 4;   forwarding-class fc10 5;   forwarding-class fc11 5;   forwarding-class fc12 6;   forwarding-class fc13 6;   forwarding-class fc14 7;   forwarding-class fc15 7; }</pre>
<b>Mapping Forwarding-Class Name to Queue Number</b>	<p>Map forwarding-class names to queue numbers:</p> <pre>[edit class-of-service] forwarding-classes {   queue 0 be;   queue 1 ef;   queue 2 af;   queue 3 nc;   queue 4 ef1;   queue 5 ef2;   queue 6 af1;   queue 7 nc1; }</pre>
<b>Mapping Diffserv Code Point Aliases to DSCP Bits</b>	<p>Map alias names to DSCP bit values. The aliases then can be used instead of the DSCP bits in adaptive services configurations.</p> <pre>[edit class-of-service] code-point-aliases {   (dscp   dscp-ipv6   exp   ieee-802.1   inet-precedence) {     alias   bits;   } }</pre>

Here is an example:

```
code-point-aliases {  
  dscp {  
    my1 110001;  
    my2 101110;  
    be 000001;  
    cs7 110000;  
  }  
}
```

**Related  
Documentation**

- [Class of Service Overview on page 82](#)
- [Restrictions and Cautions for CoS Configuration on Services Interfaces on page 716](#)
- [Configuring CoS Rules on page 717](#)
- [Configuring CoS Rule Sets on page 722](#)

## CHAPTER 28

# Summary of Class-of-Service Configuration Statements

The following sections explain each of the class-of-service (CoS) statements. The statements are organized alphabetically.

## application-profile

---

Syntax	<pre>application-profile <i>profile-name</i> {   ftp {     data {       dscp (<i>alias</i>   <i>bits</i>);       forwarding-class <i>class-name</i>;     }   }   sip {     video {       dscp (<i>alias</i>   <i>bits</i>);       forwarding-class <i>class-name</i>;     }     voice {       dscp (<i>alias</i>   <i>bits</i>);       forwarding-class <i>class-name</i>;     }   } }</pre>
Hierarchy Level	[edit <b>services</b> cos], [edit <b>services</b> cos <b>rule</b> <i>rule-name</i> <b>term</b> <i>term-name</i> <b>then</b> ], [edit <b>services</b> cos <b>rule</b> <i>rule-name</i> <b>term</b> <i>term-name</i> <b>then</b> ( <b>reflexive</b>   <b>reverse</b> )]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	Define or apply a CoS application profile. When you apply a CoS application profile in a CoS rule, terminate the profile name with a semicolon (;).
Options	<b><i>profile-name</i></b> —Identifier for the application profile.  The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Application Profiles for Use as CoS Rule Actions on page 720</a></li></ul>

## application-sets (Services CoS)

---

<b>Syntax</b>	<code>applications-sets <i>set-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Define one or more target application sets.
<b>Options</b>	<i>set-name</i> —Name of the target application set.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions In CoS Rules on page 718</a></li></ul>

## applications (Services CoS)

---

<b>Syntax</b>	<code>applications [ <i>application-name</i> ];</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Define one or more applications to which the CoS services apply.
<b>Options</b>	<i>application-name</i> —Name of the target application.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in a CoS Rule</a></li><li>• <a href="#">Configuring Match Conditions In CoS Rules on page 718</a></li></ul>

## data (FTP)

---

<b>Syntax</b>	<pre>data {     dscp (<i>alias</i>   <i>bits</i>);     forwarding-class <i>class-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit services cos <a href="#">application-profile</a> <i>profile-name</i> ftp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Set the appropriate <b>dscp</b> and <b>forwarding-class</b> value for FTP data.
<b>Default</b>	By default, the system will not alter the DSCP or forwarding class for FTP data traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Application Profiles</i></li><li>• <a href="#">video (Application Profile) on page 738</a></li><li>• <a href="#">voice (Application Profile) on page 739</a></li></ul>

## destination-address (CoS)

---

<b>Syntax</b>	<pre>destination-address (<i>address</i>   any-unicast) &lt;except&gt;;</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1. <b>address</b> option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Specify the destination address for rule matching.
<b>Options</b>	<b>address</b> —Destination IPv4 or IPv6 address or prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Match Conditions in a CoS Rule</i></li><li>• <a href="#">Configuring Match Conditions In CoS Rules on page 718</a></li></ul>

## destination-prefix-list (Services CoS)

<b>Syntax</b>	<code>destination-prefix-list <i>list-name</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	Specify the destination prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the [edit <b>policy-options</b> ] hierarchy level.
<b>Options</b>	<p><b>list-name</b>—Destination prefix list.</p> <p><b>except</b>—(Optional) Exclude the specified prefix list from rule matching.</p>
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Match Conditions In CoS Rules</a> ” on page 718.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Routing Policy Feature Guide for Routing Devices</i></li> </ul>

## dscp

<b>Syntax</b>	<code>dscp (<i>alias</i>   <i>bits</i>);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">application-profile</a> <i>profile-name</i> <a href="#">ftp</a> <a href="#">data</a> ], [edit <a href="#">services</a> cos <a href="#">application-profile</a> <i>profile-name</i> <a href="#">sip</a> ( <a href="#">video</a>   <a href="#">voice</a> )], [edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ], [edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ( <a href="#">reflexive</a>   <a href="#">reverse</a> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Define the Differentiated Services code point (DSCP) mapping that is applied to the packets.
<b>Options</b>	<p><b>alias</b>—Name assigned to a set of CoS markers.</p> <p><b>bits</b>—Mapping value in the packet header.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring Actions in CoS Rules on page 719.</a></li> </ul>

## forwarding-class

---

<b>Syntax</b>	<code>forwarding-class class-name;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">application-profile</a> <i>profile-name</i> <a href="#">ftp</a> <a href="#">data</a> ], [edit <a href="#">services</a> cos <a href="#">application-profile</a> <i>profile-name</i> <a href="#">sip</a> ( <a href="#">video</a>   <a href="#">voice</a> )], [edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ], [edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ( <a href="#">reflexive</a>   <a href="#">reverse</a> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Define the forwarding class to which packets are assigned.
<b>Options</b>	<i>class-name</i> —Name of the target application.
<b>Required Privilege Level</b>	<a href="#">interface</a> —To view this statement in the configuration. <a href="#">interface-control</a> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Actions in CoS Rules on page 719</a>.</li></ul>

## from (Services CoS)

---

<b>Syntax</b>	<pre>from {   <a href="#">application-sets</a> <i>set-name</i>;   <a href="#">applications</a> [ <i>application-names</i> ];   <a href="#">destination-address</a> (<a href="#">CoS</a>) <i>address</i>;   <a href="#">destination-prefix-list</a> <i>list-name</i> &lt;except&gt;;   <a href="#">source-address</a> <i>address</i>;   <a href="#">source-prefix-list</a> <i>list-name</i> &lt;except&gt;; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Specify input conditions for a CoS term.
<b>Options</b>	For information on match conditions, see the description of firewall filter match conditions in the <i>Routing Policy Feature Guide for Routing Devices</i> .  The remaining statements are explained separately.
<b>Required Privilege Level</b>	<a href="#">interface</a> —To view this statement in the configuration. <a href="#">interface-control</a> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring CoS Rules on page 717</a></li></ul>

## ftp (Class-Of-Service)

<b>Syntax</b>	<pre>ftp {   data {     dscp (alias   bits);     forwarding-class class-name;   } }</pre>
<b>Hierarchy Level</b>	[edit services cos <a href="#">application-profile profile-name</a> ftp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Set the appropriate <b>dscp</b> and <b>forwarding-class</b> value for FTP.
<b>Default</b>	By default, the system does not alter the DSCP or forwarding class for FTP traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Application Profiles</i></li> <li>• <a href="#">sip (Application Profile) on page 735</a></li> </ul>

## match-direction

<b>Syntax</b>	match-direction (input   output   input-output);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">rule rule-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Specify the direction in which the rule match is applied.
<b>Options</b>	<p><b>input</b>—Apply the rule match on the input side of the interface.</p> <p><b>output</b>—Apply the rule match on the output side of the interface.</p> <p><b>input-output</b>—Apply the rule match bidirectionally.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring CoS Rules</i></li> </ul>

## (reflexive | reverse)

---

<b>Syntax</b>	<pre>(reflexive   reverse) {   application-profile profile-name;   dscp (alias   bits);   forwarding-class class-name;   syslog; }</pre>
<b>Hierarchy Level</b>	[edit <b>services</b> cos <b>rule</b> rule-name <b>term</b> term-name <b>then</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	<p><b>reflexive</b>—Applies the equivalent opposing CoS action to flows in the opposite direction.</p> <p><b>reverse</b>—Allows you to define CoS behavior for flows in the reverse direction.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring CoS Rules</i></li><li>• <a href="#">Configuring Reflexive and Reverse CoS Rule Actions on page 721</a></li></ul>

## rule

<b>Syntax</b>	<pre> rule rule-name {   match-direction (input   output   input-output);   term term-name {     from {       application-sets set-name;       applications [ application-names ];       destination-address (CoS) address;       destination-prefix-list list-name &lt;except&gt;;       source-address address;       source-prefix-list list-name &lt;except&gt;;     }     then {       application-profile profile-name;       dscp (alias   bits);       forwarding-class class-name;       syslog;       (reflexive   reverse) {         application-profile profile-name;         dscp (alias   bits);         forwarding-class class-name;         syslog;       }     }   } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">services cos</a> ], [edit <a href="#">services cos rule-set</a> rule-set-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Specify the rule the router uses when applying this service.
<b>Options</b>	<p><b>rule-name</b>—Identifier for the collection of terms that constitute this rule.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring CoS Rules on page 717</a></li> </ul>

## rule-set (Services CoS)

---

<b>Syntax</b>	<code>rule-set rule-set-name {     [ <a href="#">rule rule-name</a> ]; }</code>
<b>Hierarchy Level</b>	[edit <a href="#">services cos</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<b>rule-set-name</b> —Identifier for the collection of rules that constitute this rule set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring CoS Rule Sets</a></li></ul>

## services (COS)

---

<b>Syntax</b>	<code>services cos { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Define the service rules to be applied to traffic.
<b>Options</b>	<b>cos</b> —Identifier for the class-of-service set of rules statements.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring CoS Rules on page 717</a></li></ul>

## sip (Application Profile)

<b>Syntax</b>	<pre> sip {   video {     dscp (alias   bits);     forwarding-class class-name;   }   voice {     dscp (alias   bits);     forwarding-class class-name;   } } </pre>
<b>Hierarchy Level</b>	[edit services cos <a href="#">application-profile</a> <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Set the appropriate <b>dscp</b> and <b>forwarding-class</b> value for SIP traffic.
<b>Default</b>	By default, the system will not alter the DSCP or forwarding class for SIP traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Application Profiles</i></li> <li>• <a href="#">ftp (Class-Of-Service) on page 731</a></li> </ul>

## source-address (Services CoS)

<b>Syntax</b>	source-address <i>address</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1. <b>address</b> option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Source address for rule matching.
<b>Options</b>	<b>address</b> —Source IPv4 or IPv6 address or prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Match Conditions in a CoS Rule</i></li> <li>• <a href="#">Configuring Match Conditions In CoS Rules on page 718</a></li> </ul>

## source-prefix-list

---

<b>Syntax</b>	source-prefix-list <i>list-name</i> <except>;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	Specify the source prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the [edit <b>policy-options</b> ] hierarchy level.
<b>Options</b>	<i>list-name</i> —Destination prefix list.  <b>except</b> —(Optional) Exclude the specified prefix list from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring CoS Rules on page 717</a></li><li>• <i>Routing Policy Feature Guide for Routing Devices</i></li></ul>

## syslog (Services CoS)

---

<b>Syntax</b>	syslog;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ], [edit <a href="#">services</a> cos <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">then</a> ( <a href="#">reflexive</a>   <a href="#">reverse</a> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Enable system logging. The system log information from the Adaptive Services or Multiservices PIC is passed to the kernel for logging in the <b>/var/log</b> directory. This setting overrides any <b>syslog</b> statement setting included in the service set or interface default configuration.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Actions in a CoS Rule</i></li><li>• <a href="#">Configuring Actions in CoS Rules on page 719</a></li></ul>

## term (Services CoS)

```
Syntax  term term-name {
        from {
            application-sets set-name;
            applications [ application-names ];
            destination-address (CoS) address;
            destination-prefix-list list-name <except>;
            source-address address;
            source-prefix-list list-name <except>;
        }
        then {
            application-profile profile-name;
            dscp (alias | bits);
            forwarding-class class-name;
            syslog;
            (reflexive | reverse) {
                application-profile profile-name;
                dscp (alias | bits);
                forwarding-class class-name;
                syslog;
            }
        }
    }
```

**Hierarchy Level** [edit [services](#) cos [rule](#) *rule-name*]

**Release Information** Statement introduced in Junos OS Release 8.1.

**Description** Define the CoS term properties.

**Options** *term-name*—Identifier for the term.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring CoS Rules on page 717](#).

## then

---

Syntax	<pre>then {   application-profile profile-name;   dscp (alias   bits);   forwarding-class class-name;   syslog;   (reflexive   reverse) {     application-profile profile-name;     dscp (alias   bits);     forwarding-class class-name;     syslog;   } }</pre>
Hierarchy Level	[edit <a href="#">services</a> cos <a href="#">rule</a> rule-name <a href="#">term</a> term-name]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	Define the CoS term actions.  The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring Actions in a CoS Rule</i></li><li>• <a href="#">Configuring Actions in CoS Rules on page 719</a></li></ul>

## video (Application Profile)

---

Syntax	<pre>video {   dscp (alias   bits);   forwarding-class class-name; }</pre>
Hierarchy Level	[edit services cos <a href="#">application-profile</a> profile-name sip]
Release Information	Statement introduced in Junos OS Release 9.3.
Description	Set the appropriate <b>dscp</b> and <b>forwarding-class</b> values for SIP video traffic.
Default	By default, the system will not alter the DSCP or forwarding class for SIP video traffic.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring Application Profiles</i></li><li>• <a href="#">voice (Application Profile) on page 739</a></li></ul>

## voice (Application Profile)

---

<b>Syntax</b>	<pre>voice {     dscp (<i>alias</i>   <i>bits</i>);     forwarding-class <i>class-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit services cos <a href="#">application-profile</a> <i>profile-name</i> sip]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Set the appropriate <b>dscp</b> and <b>forwarding-class</b> values for SIP voice traffic.
<b>Default</b>	By default, the system will not alter the DSCP or forwarding class for SIP voice traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Application Profiles</i></li><li>• <a href="#">video (Application Profile) on page 738</a></li></ul>



# Service Set Configuration Guidelines

A *service set* is a collection of services to be performed by an Adaptive Services (AS) or Multiservices PIC. To configure service sets, include the following statements at the **[edit services]** hierarchy level:

```
[edit services]
service-set service-set-name {
  (ids-rules rule-names | ids-rule-sets rule-set-name);
  (ipsec-vpn-rules rule-names | ipsec-vpn-rule-sets rule-set-name);
  (nat-rules rule-names | nat-rule-sets rule-set-name);
  (pgcp-rules rule-names | pgcp-rule-sets rule-set-name);
  (ptsp-rules rule-names | ptsp-rule-sets rule-set-name);
  (stateful-firewall-rules rule-names | stateful-firewall-rule-sets rule-set-name);
  allow-multicast;
  extension-service service-name {
    provider-specific rules;
  }
  interface-service {
    service-interface interface-name;
  }
  ipsec-vpn-options {
    anti-replay-window-size bits;
    clear-dont-fragment-bit;
    copy-dont-fragment-bit
    set-dont-fragment-bit
    ike-access-profile profile-name;
    local-gateway address;
    no-anti-replay;
    passive-mode-tunneling;
    trusted-ca [ ca-profile-names ];
    tunnel-mtu bytes;
  }
  max-flows number;
  next-hop-service {
    inside-service-interface interface-name.unit-number;
    outside-service-interface interface-name.unit-number;
    service-interface-pool name;
  }
  syslog {
    host hostname {
      services severity-level;
      facility-override facility-name;
    }
  }
}
```

```
        log-prefix prefix-value;  
    }  
}  
adaptive-services-pics {  
    traceoptions {  
        file filename <files number> <match regex> <size size> <(world-readable |  
        no-world-readable)>;  
        flag flag;  
    }  
}  
logging {  
    traceoptions {  
        file filename <files number> <match regex> <size size> <(world-readable |  
        no-world-readable)>;  
        flag flag;  
    }  
}
```

This chapter contains the following sections:

- [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)
- [Configuring Service Rules on page 747](#)
- [Configuring IPsec Service Sets on page 748](#)
- [Configuring Service Set Limitations on page 753](#)
- [Configuring System Logging for Service Sets on page 754](#)
- [Enabling Services PICs to Accept Multicast Traffic on page 756](#)
- [Tracing Services PIC Operations on page 756](#)
- [Example: Configuring Service Sets on page 759](#)

---

## Configuring Service Sets to be Applied to Services Interfaces

You configure a services interface to specify the adaptive services interface on which the service is to be performed. Services interfaces are used with either of the service set types described in the following sections.

- [Configuring Interface Service Sets on page 742](#)
- [Configuring Next-Hop Service Sets on page 744](#)
- [Determining Traffic Direction on page 745](#)

### Configuring Interface Service Sets

An interface service set is used as an action modifier across an entire interface. To configure the services interface, include the **interface-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level:

```
[edit services service-set service-set-name]  
interface-service {  
    service-interface interface-name;  
}
```

Only the device name is needed, because the router software manages logical unit numbers automatically. The services interface must be an adaptive services interface for which you have configured **unit 0 family inet** at the **[edit interfaces *interface-name* hierarchy level**.

When you have defined and grouped the service rules by configuring the service-set definition, you can apply services to one or more interfaces installed on the router. When you apply the service set to an interface, it automatically ensures that packets are directed to the PIC.

To associate a defined service set with an interface, include a **service-set** statement with the **input** or **output** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service]** hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet service]
input {
  service-set service-set-name <service-filter filter-name>;
  post-service-filter filter-name;
}
output {
  service-set service-set-name <service-filter filter-name>;
}
```

If a packet is entering the interface, the match direction is **input**. If a packet is leaving the interface, the match direction is **output**. The service set retains the input interface information even after services are applied, so that functions such as filter-class forwarding and destination class usage (DCU) that depend on input interface information continue to work.

You configure the same service set on the input and output sides of the interface. You can optionally include filters associated with each service set to refine the target and additionally process the traffic. If you include the **service-set** statement without a **service-filter** definition, the router software assumes the match condition is true and selects the service set for processing automatically.



**NOTE:** If you configure service sets with filters, they must be configured on the input and output sides of the interface.

You can include more than one service set definition on each side of the interface. If you include multiple service sets, the router software evaluates them in the order in which they appear in the configuration. The system executes the first service set for which it finds a match in the service filter and ignores the subsequent definitions. A maximum of six service sets can be applied to an interface. When you apply multiple service sets to an interface, you must also configure and apply a service filter to the interface.

An additional statement allows you to specify a filter for processing the traffic after the input service set is executed. To configure this type of filter, include the **post-service-filter** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service input]** hierarchy level:

```
post-service-filter filter-name;
```

The **post-service-filter** statement is not supported when the service interface is on an MS-MIC or MS-MPC.

For an example, see [“Example: Configuring Service Sets” on page 759](#).



**NOTE:** With interface-style service sets that are configured with Junos OS extension-provide packages, the traffic fails to get serviced when the ingress interface is part of a VRF instance and the service interface is not part of the same VRF instance.



**NOTE:** When the MultiServices PIC configured for a service set is either administratively taken offline or undergoes a failure, all the traffic entering the configured interface with an IDP service set would be dropped without notification. To avoid this traffic loss, include the **bypass-traffic-on-pic-failure** statement at the `[edit services service-set service-set-name service-set-options]` hierarchy level. When this statement is configured, the affected packets are forwarded in the event of a MultiServices PIC failure or offlining, as though interface-style services were not configured. This issue applies only to Junos Application Aware (previously known as Dynamic Application Awareness) configurations using IDP service sets. This forwarding feature worked only with the Packet Forwarding Engine (PFE) initially. Starting with Junos OS Release 11.3, the packet-forwarding feature is extended to packets generated by the Routing Engine for bypass service sets as well.

---

## Configuring Next-Hop Service Sets

A next-hop service set is a route-based method of applying a particular service. Only packets destined for a specific next hop are serviced by the creation of explicit static routes. This configuration is useful when services need to be applied to an entire virtual private network (VPN) routing and forwarding (VRF) table, or when routing decisions determine that services need to be performed.

When a next-hop service is configured, the AS or Multiservices PIC is considered to be a two-legged module with one leg configured to be the inside interface (inside the network) and the other configured as the outside interface (outside the network).



**NOTE:** You can create IFL indexes greater than 8000 only if the interface service set is not configured.

To configure the domain, include the **service-domain** statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

**service-domain** (inside | outside);

The **service-domain** setting must match the configuration for the next-hop service inside and outside interfaces. To configure the inside and outside interfaces, include the

**next-hop-service** statement at the **[edit services service-set service-set-name]** hierarchy level. The interfaces you specify must be logical interfaces on the same AS PIC. You cannot configure **unit 0** for this purpose, and the logical interface you choose must not be used by another service set.

```
next-hop-service {
  inside-service-interface interface-name.unit-number;
  outside-service-interface interface-name.unit-number;
}
```

Traffic on which the service is applied is forced to the inside interface using a static route. For example:

```
routing-options {
  static {
    route 10.1.2.3 next-hop sp-1/1/0.1;
  }
}
```

After the service is applied, traffic exits by way of the outside interface. A lookup is then performed in the Packet Forwarding Engine (PFE) to send the packet out of the AS or Multiservices PIC.

The reverse traffic enters the outside interface, is serviced, and sent to the inside interface. The inside interface forwards the traffic out of the AS or Multiservices PIC.

## Determining Traffic Direction

When you configure next-hop service sets, the AS PIC functions as a two-part interface, in which one part is the *inside* interface and the other part is the *outside* interface. The following sequence of actions takes place:

1. To associate the two parts with logical interfaces, you configure two logical interfaces with the **service-domain** statement, one with the **inside** value and one with the **outside** value, to mark them as either an inside or outside service interface.
2. The router forwards the traffic to be serviced to the inside interface, using the next-hop lookup table.
3. After the service is applied, the traffic exits from the outside interface. A route lookup is then performed on the packets to be sent out of the router.
4. When the reverse traffic returns on the outside interface, the applied service is undone; for example, IPsec traffic is decrypted or NAT addresses are unmasked. The serviced packets then emerge on the inside interface, the router performs a route lookup, and the traffic exits the router.

A service rule's match direction, whether input, output, or input/output, is applied with respect to the traffic flow through the AS PIC, not through a specific inside or outside interface.

When a packet is sent to an AS PIC, packet direction information is carried along with it. This is true for both interface style and next-hop style service sets.

### Interface Style Service Sets

---

Packet direction is determined by whether a packet is entering or leaving any Packet Forwarding Engine interface (with respect to the forwarding plane) on which the **interface-service** statement is applied. This is similar to the input and output direction for stateless firewall filters.

The match direction can also depend on the network topology. For example, you might route all the external traffic through one interface that is used to protect the other interfaces on the router, and configure various services on this interface specifically. Alternatively, you might use one interface for priority traffic and configure special services on it, but not care about protecting traffic on the other interfaces.

### Next-Hop Style Service Sets

---

Packet direction is determined by the AS PIC interface used to route packets to the AS PIC. If you use the **inside-interface** statement to route traffic, then the packet direction is **input**. If you use the **outside-interface** statement to direct packets to the AS PIC, then the packet direction is **output**.

The interface to which you apply the service sets affects the match direction. For example, apply the following configuration:

```
sp-1/1/0 unit 1 service-domain inside;  
sp-1/1/0 unit 2 service-domain outside;
```

If you configure **match-direction input**, you include the following statements:

```
[edit]  
services service-set test1 next-hop-service inside-service-interface sp-1/0/0.1;  
services service-set test1 next-hop-service outside-service-interface sp-1/0/0.2;  
services ipsec-vpn rule test-ipsec-rule match-direction input;  
routing-options static route 10.0.0.0/24 next-hop sp-1/1/0.1;
```

If you configure **match-direction output**, you include the following statements:

```
[edit]  
services service-set test2 next-hop-service inside-service-interface sp-1/0/0.1;  
services service-set test2 next-hop-service outside-service-interface sp-1/0/0.2;  
services ipsec-vpn rule test-ipsec-rule match-direction output;  
routing-options static route 10.0.0.0/24 next-hop sp-1/1/0.2;
```

The essential difference between the two configurations is the change in the match direction and the static routes' next hop, pointing to either the AS PIC's inside or outside interface.

#### Related Documentation

- [Understanding Service Sets](#)
- [Configuring Service Rules on page 747](#)
- [Configuring IPsec Service Sets on page 748](#)
- [Configuring Service Set Limitations on page 753](#)
- [Configuring System Logging for Service Sets on page 754](#)

- [Example: Configuring Service Sets on page 759](#)

## Configuring Service Rules

You specify the collection of rules and rule sets that constitute the service set. The router performs rule sets in the order in which they appear in the configuration. You can include only one rule set for each service type. You configure the rule names and content for each service type at the **[edit services *name*]** hierarchy level for each type:

- You configure intrusion detection service (IDS) rules at the **[edit services *ids*]** hierarchy level; for more information, see [“Configuring IDS Rules” on page 447](#).
- You configure IP Security (IPsec) rules at the **[edit services *ipsec-vpn*]** hierarchy level; for more information, see *Junos VPN Site Secure..*
- You configure Network Address Translation (NAT) rules at the **[edit services *nat*]** hierarchy level; for more information, see *Junos Address Aware Carrier Grade NAT and IPv6 Feature Guide..*
- You configure packet-triggered subscribers and policy control (PTSP) rules at the **[edit services *ptsp*]** hierarchy level; for more information, see *Packet-Triggered Subscribers and Policy Control Feature Guide*.
- You configure software rules for DS-Lite or 6rd softwires at the **[edit services *software*]** hierarchy level; for more information, see *Software Services*.
- You configure stateful firewall rules at the **[edit services *stateful-firewall*]** hierarchy level; for more information, see *Junos Network Secure*.

To configure the rules and rule sets that constitute a service set, include the following statements at the **[edit services *service-set* *service-set-name*]** hierarchy level:

```
([ ids-rules rule-names ] | ids-rule-sets rule-set-name);
([ ipsec-vpn-rules rule-names ] | ipsec-vpn-rule-sets rule-set-name);
([ nat-rules rule-names ] | nat-rule-sets rule-set-name);
([ pgcp-rules rule-names ] | pgcp-rule-sets rule-set-name);
([ software-rules rule-names ] | software-rule-sets rule-set-name);
([ stateful-firewall-rules rule-names ] | stateful-firewall-rule-sets rule-set-name);
```

For each service type, you can include one or more individual rules, or one rule set.

If you configure a service set with IPsec rules, it must not contain rules for any other services. You can, however, configure another service set containing rules for the other services and apply both service sets to the same interface.



**NOTE:** You can also include Junos Application Aware (previously known as Dynamic Application Awareness) functionality within service sets. To do this, you must include an `idp-profile` statement at the `[edit services service-set]` hierarchy level, along with application identification (APPID) rules, and, as appropriate, application-aware access list (AACL) rules and a `policy-decision-statistics-profile`. Only one service sets can be applied to a single interface when Junos Application Aware functionality is used. For more information, see *Intrusion Detection and Prevention*, *Application Identification*, and *Application-Aware Access List*.

- Related Documentation**
- [Understanding Service Sets](#)
  - [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)
  - [Configuring Service Set Limitations on page 753](#)
  - [Configuring System Logging for Service Sets on page 754](#)

---

## Configuring IPsec Service Sets

IPsec service sets require additional specifications that you configure at the `[edit services service-set service-set-name ipsec-vpn-options]` hierarchy level:

```
[edit services service-set service-set-name ipsec-vpn-options]
anti-replay-window-size bits;
clear-dont-fragment-bit;
copy-dont-fragment-bit
set-dont-fragment-bit
ike-access-profile profile-name;
local-gateway address;
no-anti-replay;
passive-mode-tunneling;
trusted-ca [ ca-profile-names ];
tunnel-mtu bytes;
```

Configuration of these statements is described in the following sections:

- [Configuring the Local Gateway Address for IPsec Service Sets on page 748](#)
- [Configuring IKE Access Profiles for IPsec Service Sets on page 750](#)
- [Configuring Certification Authorities for IPsec Service Sets on page 750](#)
- [Configuring or Disabling Antireplay Service on page 750](#)
- [Clearing the Don't-Fragment Bit on page 751](#)
- [Configuring Passive-Mode Tunneling on page 752](#)
- [Configuring the Tunnel MTU Value on page 752](#)

### Configuring the Local Gateway Address for IPsec Service Sets

If you configure an IPsec service set, you must also configure a local IPv4 or IPv6 address by including the `local-gateway` statement:

- If the Internet Key Exchange (IKE) gateway IP address is in **inet.0** (the default situation), you configure the following statement:

**local-gateway** *address*;

- If the IKE gateway IP address is in a VPN routing and forwarding (VRF) instance, you configure the following statement:

**local-gateway** *address* routing-instance *instance-name*;

You can configure all the link-type tunnels that share the same local gateway address in a single next-hop-style service set. The value you specify for the **inside-service-interface** statement at the **[edit services service-set service-set-name]** hierarchy level should match the **ipsec-inside-interface** value, which you configure at the **[edit services ipsec-vpn rule rule-name term term-name from]** hierarchy level. For more information about IPsec configuration, see [“Configuring IPsec Rules” on page 504](#).

### IKE Addresses in VRF Instances

You can configure Internet Key Exchange (IKE) gateway IP addresses that are present in a VPN routing and forwarding (VRF) instance as long as the peer is reachable through the VRF instance.

For next-hop service sets, the key management process (kmd) places the IKE packets in the routing instance that contains the **outside-service-interface** value you specify, as in this example:

```
routing-instances vrf-nxthop {
  instance-type vrf;
  interface sp-1/1/0.2;
  ...
}
services service-set service-set-1 {
  next-hop-service {
    inside-service-interface sp-1/1/0.1;
    outside-service-interface sp-1/1/0.2;
  }
  ...
}
```

For interface service sets, the **service-interface** statement determines the VRF, as in this example:

```
routing-instances vrf-intf {
  instance-type vrf;
  interface sp-1/1/0.3;
  interface ge-1/2/0.1; # interface on which service set is applied
  ...
}
services service-set service-set-2 {
  interface-service {
    service-interface sp-1/1/0.3;
  }
  ...
}
```

## Configuring IKE Access Profiles for IPsec Service Sets

For dynamic endpoint tunneling only, you need to reference the IKE access profile configured at the **[edit access]** hierarchy level. To do this, include the **ike-access-profile** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level:

```
[edit services service-set service-set-name ipsec-vpn-options]
ike-access-profile profile-name;
```

The **ike-access-profile** statement must reference the same name as the **profile** statement you configured for IKE access at the **[edit access]** hierarchy level. You can reference only one access profile in each service set. This profile is used to negotiate IKE and IPsec security associations with dynamic peers only.



**NOTE:** If you configure an IKE access profile in a service set, no other service set can share the same local-gateway address.

Also, you must configure a separate service set for each VRF. All interfaces referenced by the **ipsec-inside-interface** statement within a service set must belong to the same VRF.

---

## Configuring Certification Authorities for IPsec Service Sets

You can specify one or more trusted certification authorities by including the **trusted-ca** statement:

```
trusted-ca [ ca-profile-names ];
```

When you configure public key infrastructure (PKI) digital certificates in the IPsec configuration, each service set can have its own set of trusted certification authorities. The names you specify for the **trusted-ca** statement must match profiles configured at the **[edit security pki]** hierarchy level; for more information, see the *Junos OS Administration Library for Routing Devices*. For more information about IPsec digital certificate configuration, see “Configuring IPsec Rules” on page 504.

## Configuring or Disabling Antireplay Service

You can include the **anti-replay-window-size** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level to specify the size of the antireplay window.

```
anti-replay-window-size bits;
```

This statement is useful for dynamic endpoint tunnels for which you cannot configure the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.

For static IPsec tunnels, this statement sets the antireplay window size for all the static tunnels within this service set. If a particular tunnel needs a specific value for antireplay window size, set the **anti-replay-window-size** statement at the **[edit services ipsec-vpn**

**rule rule-name term term-name then**] hierarchy level. If antireplay check has to be disabled for a particular tunnel in this service set, set the **no-anti-replay** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.



**NOTE:** The anti-replay-window-size and no-anti-replay settings at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level override the settings specified at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level.

You can also include the **no-anti-replay** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level to disable IPsec antireplay service. It occasionally causes interoperability issues for security associations.

```
no-anti-replay;
```

This statement is useful for dynamic endpoint tunnels for which you cannot configure the **no-anti-reply** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.

For static IPsec tunnels, this statement disables the antireplay check for all the tunnels within this service set. If antireplay check has to be enabled for a particular tunnel, then set the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.



**NOTE:** Setting the anti-replay-window-size and no-anti-replay statements at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level overrides the settings specified at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level.

## Clearing the Don't-Fragment Bit

You can include the **clear-dont-fragment-bit** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level to clear the Don't Fragment (DF) bit on all IP version 4 (IPv4) packets entering the IPsec tunnel. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation.

```
clear-dont-fragment-bit;
```

This statement is useful for dynamic endpoint tunnels, for which you cannot configure the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.

For static IPsec tunnels, setting this statement clears the DF bit on packets entering all the static tunnels within this service set. If you want to clear the DF bit on packets entering a specific tunnel, set the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.

In packets that are transmitted through dynamic endpoint IPsec tunnels, you can enable the value set in the Don't Fragment (DF) bit of the packet entering the tunnel to be copied only to the outer header of the IPsec packet and to not cause any modification to the DF bit in the inner header of the IPsec packet. If the packet size exceeds the tunnel maximum transmission unit (MTU) value, the packet is fragmented before encapsulation. For IPsec tunnels, the default MTU value is 1500 regardless of the interface MTU setting. To copy the DF bit value to only the outer header and not modify the inner header, use the **copy-dont-fragment-bit** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level. You can also configure the DF bit to be set only in the outer IPv4 header of the IPsec packet and not be defined in the inner IPv4 header. To configure the DF bit in only the outer header of the IPsec packet and to leave the inner header unmodified, include the **set-dont-fragment-bit** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level. These settings apply for dynamic endpoint tunnels and not for static tunnels, for which you need to include the **copy-dont-fragment-bit** and **set-dont-fragment-bit** statements at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level to clear the DF bit in the IPv4 packets that enter the static tunnel. These functionalities are supported on MX Series routers with MS-MICs and MS-MPCs.

## Configuring Passive-Mode Tunneling

You can include the **passive-mode-tunneling** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level to enable the service set to tunnel malformed packets.

```
[edit services service-set service-set-name ipsec-vpn-options]
passive-mode-tunneling;
```

This functionality bypasses the active IP checks, such as version, TTL, protocol, options, address and other land attack checks, and tunnels the packets as is. If this statement is not configured, packets failing the IP checks are dropped in the PIC. In passive mode, the inner packet is not touched; hence, an ICMP error is not generated, if the packet size exceeds the tunnel MTU value.

The IPsec tunnel is not treated as a next hop and TTL is not decremented. Because an ICMP error is not generated if the packet size exceeds the tunnel MTU value, the packet will be tunnelled even if it crosses the tunnel MTU threshold.



**NOTE:** This functionality is similar to that provided by the **no-ipsec-tunnel-in-traceroute** statement, described in [“Disabling IPsec Tunnel Endpoint in Traceroute” on page 518](#).

## Configuring the Tunnel MTU Value

You can include the **tunnel-mtu** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level to set the maximum transmission unit (MTU) value for IPsec tunnels.

```
tunnel-mtu bytes;
```

This statement is useful for dynamic endpoint tunnels for which you cannot configure the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.

For static IPsec tunnels, this statement sets the tunnel MTU value for all the tunnels within this service set. If you need a specific value for a particular tunnel, then set the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level.



**NOTE:** The **tunnel-mtu** setting at the **[edit services ipsec-vpn rule rule-name term term-name then]** hierarchy level overrides the value specified at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level.

#### Related Documentation

- [Understanding Service Sets](#)
- [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)
- [Configuring Service Set Limitations on page 753](#)
- [Configuring System Logging for Service Sets on page 754](#)

## Configuring Service Set Limitations

You can set the following limitations on service set capacity:

- You can limit the maximum number of flows allowed per service set. To configure the maximum value, include the **max-flows** statement at the **[edit services service-set service-set-name]** hierarchy level:

**max-flows** *number*;

The **max-flows** statement permits you to assign a single flow limit value. For IDS service sets only, you can specify various types of flow limits with a finer degree of control. For more information, see the description of the **session-limit** statement in “[Configuring IDS Rule Sets](#)” on page 453.



**NOTE:** When an aggregated multiservices (AMS) interface is configured as the service interface for a service set, the **max-flow** value configured for the service set is applied to each of the member interfaces in the AMS interface. That is, if you have configured 1000 as the **max-flow** value for a service set that uses an AMS interface with four active member interfaces, each of the member interfaces can handle 1000 flows each, resulting in an effective **max-flow** value of 4000.

- You can limit the maximum segment size (MSS) allowed by the Transmission Control Protocol (TCP). To configure the maximum value, include the **tcp-mss** statement at the **[edit services service-set service-set-name]** hierarchy level:

**tcp-mss** *number*;

The TCP protocol negotiates an MSS value during session connection establishment between two peers. The MSS value negotiated is primarily based on the MTU of the interfaces to which the communicating peers are directly connected to. However in the network, due to variation in link MTU on the path taken by the TCP packets, some packets which are still well within the MSS value may be fragmented when the concerned packet's size exceeds the link's MTU.

If the router receives a TCP packet with the SYN bit and MSS option set and the MSS option specified in the packet is larger than the MSS value specified by the **tcp-mss** statement, the router replaces the MSS value in the packet with the lower value specified by the **tcp-mss** statement. The range for the **tcp-mss mss-value** parameter is from **536** through **65535**.

To view statistics of SYN packets received and SYN packets whose MSS value, is modified, issue the **show services service-sets statistics tcp-mss** operational mode command. For more information on this topic, see the *Junos OS Administration Library for Routing Devices*.

**Related  
Documentation**

- [Understanding Service Sets](#)
- [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)
- [Configuring Service Rules on page 747](#)
- [Configuring System Logging for Service Sets on page 754](#)
- [Configuring SNMP Traps for Flow Limits](#)

---

## Configuring System Logging for Service Sets

---

You specify properties that control how system log messages are generated for the service set. These values override the values configured at the **[edit interfaces interface-name services-options]** hierarchy level.

To configure service-set-specific system logging values, include the **syslog** statement at the **[edit services service-set service-set-name]** hierarchy level:

```
syslog {  
  host hostname {  
    class class-name  
    facility-override facility-name;  
    log-prefix prefix-value;  
    port port-number  
    services severity-level;  
    source-address source-address  
  }  
}
```

Configure the **host** statement with a hostname or an IP address that specifies the system log target server. The hostname **local** directs system log messages to the Routing Engine. For external system log servers, the hostname must be reachable from the same routing instance to which the initial data packet (that triggered session establishment) is

delivered. You can specify only one system logging hostname. The **source-address** parameter is supported on the ms, rms, and mams interfaces.

Table 31 on page 755 lists the severity levels that you can specify in configuration statements at the **[edit services service-set service-set-name syslog host hostname]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

**Table 31: System Log Message Severity Levels**

Severity Level	Description
<b>any</b>	Includes all severity levels
<b>emergency</b>	System panic or other condition that causes the router to stop functioning
<b>alert</b>	Conditions that require immediate correction, such as a corrupted system database
<b>critical</b>	Critical conditions, such as hard drive errors
<b>error</b>	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
<b>warning</b>	Conditions that warrant monitoring
<b>notice</b>	Conditions that are not errors but might warrant special handling
<b>info</b>	Events or non-error conditions of interest

We recommend setting the system logging severity level to **error** during normal operation. To monitor PIC resource usage, set the level to **warning**. To gather information about an intrusion attack when an intrusion detection system error is detected, set the level to **notice** for a specific service set. To debug a configuration or log NAT functionality, set the level to **info**.

For more information about system log messages, see the *Junos OS System Log Messages Reference*.

To select the class of messages to be logged to the specified system log host, include the **class** statement at the **[edit services service-set service-set-name syslog host hostname]** hierarchy level:

```
class class-name;
```

To use one particular facility code for all logging to the specified system log host, include the **facility-override** statement at the **[edit services service-set service-set-name syslog host hostname]** hierarchy level:

```
facility-override facility-name;
```

The supported facilities are: **authorization**, **daemon**, **ftp**, **kernel**, **user**, and **local0** through **local7**.

To specify a text prefix for all logging to this system log host, include the **log-prefix** statement at the **[edit services service-set service-set-name syslog host hostname]** hierarchy level:

**log-prefix** *prefix-value*;

**Related  
Documentation**

- [Understanding Service Sets](#)
- [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)
- [Tracing Services PIC Operations on page 756](#)

---

## Enabling Services PICs to Accept Multicast Traffic

To allow multicast traffic to be sent to the Adaptive Services or Multiservices PIC, include the **allow-multicast** statement at the **[edit services service-set service-set-name]** hierarchy level. If this statement is not included, multicast traffic is dropped by default. This statement applies only to multicast traffic using a next-hop service set; interface service set configuration is not supported. Only unidirectional flows are created for multicast packets.

**Related  
Documentation**

- [Understanding Service Sets](#)
- [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)
- [Configuring Service Rules on page 747](#)
- [Example: Configuring Service Sets on page 759](#)
- [Example: Configuring NAT for Multicast Traffic on page 247](#)

---

## Tracing Services PIC Operations

Tracing operations track all adaptive services operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

By default, no events are traced. If you include the **traceoptions** statement at the **[edit services adaptive-services-pics]** or **[edit services logging]** hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called **serviced** located in the **/var/log** directory.
- When the file **serviced** reaches 128 kilobytes (KB), it is renamed **serviced.0**, then **serviced.2**, and so on, until there are three trace files. Then the oldest trace file (**serviced.2**) is overwritten. (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory (**/var/log**) in which trace files are located. However, you can customize the other trace file settings by including the following statements:

```

file filename <files number> <match regular-expression> <size size> <world-readable |
no-world-readable>;
flag {
  all;
  command-queued;
  config;
  handshake;
  init;
  interfaces;
  mib;
  removed-client;
  show;
}

```

You include these statements at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level.

These statements are described in the following sections:

- [Configuring the Adaptive Services Log Filename on page 757](#)
- [Configuring the Number and Size of Adaptive Services Log Files on page 757](#)
- [Configuring Access to the Log File on page 758](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 758](#)
- [Configuring the Trace Operations on page 758](#)

## Configuring the Adaptive Services Log Filename

By default, the name of the file that records trace output is **serviced**. You can specify a different name by including the **file** statement at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file filename;
```

## Configuring the Number and Size of Adaptive Services Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed **filename.0**, then **filename.1**, and so on, until there are three trace files. Then the oldest trace file (**filename.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file <filename> files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (**filename**) reaches 2 MB, **filename** is renamed **filename.0**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0** is renamed **filename.1** and **filename** is renamed **filename.0**. This process repeats until there are 20 trace files. Then the oldest file (**filename.19**) is overwritten by the newest file (**filename.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

## Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file <filename> world-readable;
```

To explicitly set the default behavior, include the **file no-world-readable** statement at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file <filename> no-world-readable;
```

## Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including the **match** statement at the **[edit services adaptive-services-pics traceoptions file filename]** or **[edit services logging traceoptions]** hierarchy level and specifying a regular expression (regex) to be matched:

```
file <filename> match regular-expression;
```

## Configuring the Trace Operations

By default, if the **traceoptions** configuration is present, only important events are logged. You can configure the trace operations to be logged by including the following statements at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
flag {
  all;
  configuration;
  routing-protocol;
  routing-socket;
  snmp;
}
```

Table 32 on page 758 describes the meaning of the adaptive services tracing flags.

**Table 32: Adaptive Services Tracing Flags**

Flag	Description	Default Setting
<b>all</b>	Trace all operations.	Off
<b>command-queued</b>	Trace command enqueue events.	Off
<b>config</b>	Log reading of the configuration at the <b>[edit services]</b> hierarchy level.	Off

Table 32: Adaptive Services Tracing Flags (*continued*)

Flag	Description	Default Setting
<b>handshake</b>	Trace handshake events.	Off
<b>init</b>	Trace initialization events.	Off
<b>interfaces</b>	Trace interface events.	Off
<b>mib</b>	Trace GGSN SNMP MIB events.	Off
<b>removed-client</b>	Trace client cleanup events.	Off
<b>show</b>	Trace CLI command servicing.	Off

To display the end of the log, issue the **show log serviced | last** operational mode command:

```
[edit]
user@host# run show log serviced | last
```

#### Related Documentation

- [Understanding Service Sets](#)
- [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)
- [Configuring System Logging for Service Sets on page 754](#)

## Example: Configuring Service Sets

Apply two service sets, **my-input-service-set** and **my-output-service-set**, on an interface-wide basis. All traffic has **my-input-service-set** applied to it. After the service set is applied, additional filtering is done using **my\_post\_service\_input\_filter**.

```
[edit interfaces fe-0/1/0]
unit 0 {
  family inet {
    service {
      input {
        service-set my-input-service-set;
        post-service-filter my_post_service_input_filter;
      }
      output {
        service-set my-output-service-set;
      }
    }
  }
}
```

#### Related Documentation

- [Understanding Service Sets](#)
- [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)



# Summary of Service Set Configuration Statements

The following sections explain each of the service set configuration statements. The statements are organized alphabetically.

- [adaptive-services-pics](#) on page 762
- [allow-multicast](#) on page 763
- [anti-replay-window-size](#) (Services Service Set) on page 764
- [bypass-traffic-on-exceeding-flow-limits](#) on page 765
- [bypass-traffic-on-pic-failure](#) on page 765
- [clear-dont-fragment-bit](#) (Services Service Set) on page 766
- [copy-dont-fragment-bit](#) (Services Set) on page 767
- [facility-override](#) on page 768
- [host](#) (service-set) on page 769
- [ids-rules](#) on page 770
- [ike-access-profile](#) on page 770
- [interface-service](#) on page 771
- [ip-reassembly-rules](#) (Service Set) on page 771
- [ipsec-vpn-options](#) on page 772
- [ipsec-vpn-rules](#) on page 772
- [local-gateway](#) on page 773
- [log-prefix](#) (Services) on page 773
- [logging](#) (Services) on page 774
- [max-flows](#) on page 775
- [message-rate-limit](#) on page 776
- [nat-options](#) on page 777
- [nat-rules](#) on page 777
- [next-hop-service](#) on page 778
- [no-anti-replay](#) (Services Service Set) on page 779

- [passive-mode-tunneling](#) on page 780
- [pgcp-rules](#) on page 780
- [port \(syslog\)](#) on page 781
- [ptsp-rules](#) on page 781
- [service-interface](#) on page 782
- [service-set \(Services\)](#) on page 783
- [service-set-options](#) on page 785
- [softwire-options](#) on page 785
- [set-dont-fragment-bit \(Services Set\)](#) on page 788
- [stateful-firewall-rules](#) on page 788
- [syslog \(Services Service Set\)](#) on page 789
- [tcp-mss](#) on page 790
- [traceoptions \(Services Logging\)](#) on page 791
- [trusted-ca](#) on page 792
- [tunnel-mtu \(Services Service Set\)](#) on page 793

---

## **adaptive-services-pics**

---

<b>Syntax</b>	<pre>adaptive-services-pics {   <a href="#">traceoptions</a> {     file <i>filename</i> &lt;files number&gt; &lt;match regular-expression&gt; &lt;size size&gt; &lt;world-readable         no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace;   } }</pre>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. The <b>file</b> option was added in Release 8.0.
<b>Description</b>	Define global services properties.
<b>Options</b>	The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	• <a href="#">Tracing Services PIC Operations</a> on page 756


## allow-multicast

---

<b>Syntax</b>	allow-multicast;
<b>Hierarchy Level</b>	[edit services <a href="#">service-set</a> <i>service-set-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.0.
<b>Description</b>	Allow multicast traffic to be sent to the Adaptive Services or Multiservices PIC.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Enabling Services PICs to Accept Multicast Traffic on page 756</a></li></ul>

## anti-replay-window-size (Services Service Set)

---

<b>Syntax</b>	<code>anti-replay-window-size <i>bits</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> service-set <i>service-set-name</i> ipsec-vpn-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	<p>Specify the size of the IPsec antireplay window. This statement is useful for dynamic endpoint tunnels for which you cannot configure the <b>anti-replay-window-size</b> statement at the [edit <a href="#">services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</a>] hierarchy level.</p> <p>For static IPsec tunnels, this statement sets the antireplay window size for all the static tunnels within this service set. If a particular tunnel needs a specific value for antireplay window size, set the <b>anti-replay-window-size</b> statement at the [edit <a href="#">services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</a>] hierarchy level. If antireplay check has to be disabled for a particular tunnel in this service set, set the <b>no-anti-replay</b> statement at the [edit <a href="#">services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</a>] hierarchy level.</p>
	<div> <b>NOTE:</b> The anti-replay-window-size and no-anti-replay settings at the [edit <a href="#">services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</a>] hierarchy level override the settings specified at the [edit <a href="#">services service-set <i>service-set-name</i> ipsec-vpn-options</a>] hierarchy level.</div>
<b>Options</b>	<p><b>bits</b>—Size of the antireplay window, in bits.</p> <p><b>Default:</b> 64 bits (AS PICs), 128 bits (Multiservices PICs and DPCs)</p> <p><b>Range:</b> 64 through 4096 bits</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IPsec Service Sets on page 748</a></li><li>• <a href="#">Configuring or Disabling IPsec Anti-Replay on page 510</a></li></ul>

## bypass-traffic-on-exceeding-flow-limits

---

<b>Syntax</b>	bypass-traffic-on-exceeding-flow-limits;
<b>Hierarchy Level</b>	[edit <b>services</b> service-set <i>service-set-name</i> service-set-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Enable packets to bypass without creating a new session when the flow in the service set exceeds the limit that is set by the <b>max-flows</b> statement at the [edit <b>services</b> service-set <i>service-set-name</i> ] hierarchy level.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li> </ul>

## bypass-traffic-on-pic-failure

---

<b>Syntax</b>	bypass-traffic-on-pic-failure;
<b>Hierarchy Level</b>	[edit <b>services</b> service-set <i>service-set-name</i> service-set-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	<p>When the MultiServices PIC configured for a service set is either administratively taken offline or undergoes a failure, all the traffic entering the configured interface with an IDP service set would be dropped without notification. To avoid this traffic loss, include the <b>bypass-traffic-on-pic-failure</b> statement. When this statement is configured, the affected packets are forwarded in the event of a MultiServices PIC failure or offlining, as though interface-style services were not configured.</p> <p>This issue applies only to Junos Application Aware (previously known as Dynamic Application Awareness) configurations with IDP service sets.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li> </ul>

## clear-dont-fragment-bit (Services Service Set)

---

<b>Syntax</b>	clear-dont-fragment-bit;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> service-set <i>service-set-name</i> ipsec-vpn-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	<p>Clear the Don't Fragment (DF) bit on all IP version 4 (IPv4) packets entering the IPsec tunnel. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. This statement is useful for dynamic endpoint tunnels, for which you cannot configure the <b>clear-dont-fragment-bit</b> statement at the [edit <a href="#">services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</a>] hierarchy level.</p> <p>For static IPsec tunnels, setting this statement clears the DF bit on packets entering all the static tunnels within this service set. If you want to clear the DF bit on packets entering a specific tunnel, set the <b>clear-dont-fragment-bit</b> statement at the [edit <a href="#">services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</a>] hierarchy level.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IPsec Service Sets on page 748</a></li><li>• <a href="#">Configuring Actions in IPsec Rules on page 508</a></li></ul>

## copy-dont-fragment-bit (Services Set)

<b>Syntax</b>	copy-dont-fragment-bit;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> service-set <i>service-set-name</i> ipsec-vpn-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Copy the do not fragment (DF) bit value to only the outer header and not modify the inner header of the IPsec packet in dynamic endpoint tunnels. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs. These settings apply for dynamic endpoint tunnels and not for static tunnels, for which you need to include the <b>copy-dont-fragment-bit</b> statement at the [edit <b>services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</b> ] hierarchy level to copy the DF bit value to only the outer header of the packet in a static IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring IPsec Service Sets on page 748</a></li> <li>• <a href="#">Configuring Actions in IPsec Rules on page 508</a></li> </ul>

## facility-override

---

<b>Syntax</b>	<code>facility-override <i>facility-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name syslog host hostname</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Override the default facility for system log reporting.
<b>Options</b>	<p><i>facility-name</i>—Name of the facility that overrides the default assignment. Valid entries are:</p> <ul style="list-style-type: none"><li><code>authorization</code></li><li><code>daemon</code></li><li><code>ftp</code></li><li><code>kernel</code></li><li><code>local0</code> through <code>local7</code></li><li><code>user</code></li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Logging for Service Sets on page 754</a></li></ul>

## host (service-set)

<b>Syntax</b>	<pre> host <i>hostname</i> {   class {     alg-logs;     ids-logs;     nat-logs;     packet-logs;     pcp-logs;     session-logs &lt;open   close&gt;;     stateful-firewall-logs ;   }   <b>facility-override</b> <i>facility-name</i>;   <b>interface-service</b> <i>prefix-value</i>;   <b>log-prefix</b><i>prefix-value</i>   <b>port</b> <i>port-number</i>   <b>services</b> <i>severity-level</i>;   <b>source-address</b><i>source-address</i> } </pre>
<b>Hierarchy Level</b>	[edit <b>services service-set</b> <i>service-set-name syslog</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. <b>class</b> option introduced in Junos OS Release 13.2.
<b>Description</b>	Specify the hostname for the system logging utility.
<b>Options</b>	<p><b>hostname</b>—Name of the system logging utility host machine.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring System Logging for Service Sets on page 754</a></li> </ul>

## ids-rules

---

<b>Syntax</b>	(ids-rules <i>rule-name</i>   ids-rule-sets <i>rule-set-name</i> );
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the intrusion detection service (IDS) rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.
<b>Options</b>	<i>rule-name</i> —Identifier for the collection of terms that constitute this rule. <i>rule-set-name</i> —Identifier for the set of rules to be included.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Rules on page 747</a></li></ul>

## ike-access-profile

---

<b>Syntax</b>	ike-access-profile <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name ipsec-vpn-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Define the access profile for the IPsec traffic on dynamic tunnels.
<b>Options</b>	<i>profile-name</i> —Identifier for access profile, which must match the name configured at the [edit access profile <i>name</i> client * ike] hierarchy level.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Dynamic Endpoints for IPsec Tunnels on page 512</a></li><li>• <a href="#">Configuring IPsec Service Sets on page 748</a></li></ul>

## interface-service

<b>Syntax</b>	interface-service { service-interface <i>name</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the device name for the interface service Physical Interface Card (PIC).
<b>Options</b>	<b>service-interface <i>name</i></b> —Name of the service device associated with the interface-wide service set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li> </ul>

## ip-reassembly-rules (Service Set)

<b>Syntax</b>	ip-reassembly-rules <i>rule-name</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.1.
<b>Description</b>	Specify one or more previously configured IP reassembly rules to associate with the service set.



**NOTE:** The IP reassembly rule must be defined at the [edit services ip-reassembly rule] hierarchy level.

<b>Options</b>	<b><i>rule-name</i></b> —Name of an IP reassembly rule.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring IP Inline Reassembly for L2TP on page 590</a></li> <li>• <a href="#">IP Packet Fragment Reassembly for L2TP Overview on page 589</a></li> </ul>

## ipsec-vpn-options

---

Syntax	<pre>ipsec-vpn-options {   anti-replay-window-size <i>bits</i>;   clear-dont-fragment-bit;   ike-access-profile <i>profile-name</i>;   local-gateway <i>address</i>;   no-anti-replay;   passive-mode-tunneling;   trusted-ca [ <i>ca-profile-names</i> ];   tunnel-mtu <i>bytes</i>; }</pre>
Hierarchy Level	[edit <a href="#">services service-set service-set-name</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify IP Security (IPsec) service options.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Rules on page 747</a></li></ul>

## ipsec-vpn-rules

---

Syntax	<pre>(ipsec-vpn-rules <i>rule-name</i>   ipsec-vpn-rule-sets <i>rule-set-name</i>);</pre>
Hierarchy Level	[edit <a href="#">services service-set service-set-name</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the IPsec rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.
Options	<i>rule-name</i> —Identifier for the collection of terms that constitute this rule.  <i>rule-set-name</i> —Identifier for the set of rules to be included.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Rules on page 747</a></li></ul>

## local-gateway

---

<b>Syntax</b>	<code>local-gateway <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name ipsec-vpn-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the local IPv4 or IPv6 address for the IPsec traffic.
<b>Options</b>	<i>address</i> —Local address.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Rules on page 747</a></li></ul>

## log-prefix (Services)

---


<b>Syntax</b>	<code>log-prefix <i>prefix-value</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name syslog host hostname</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Set the system logging prefix value.
<b>Options</b>	<i>prefix-value</i> —System logging prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Logging for Service Sets on page 754</a></li></ul>

## logging (Services)


---

<b>Syntax</b>	<pre>logging {   traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable         no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace;   } }</pre>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.0.
<b>Description</b>	Define global services properties.
<b>Options</b>	The remaining statement is explained separately.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Tracing Services PIC Operations on page 756</a></li></ul>

## max-flows

<b>Syntax</b>	<code>max-flows <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Maximum number of flows allowed for the service set.
<b>Options</b>	<i>number</i> —Maximum number of flows.
<div>  <p><b>NOTE:</b> When an aggregated multiservices (AMS) interface is configured as the service interface for a service set, the max-flow value configured for the service set is applied to each of the member interfaces in the AMS interface. That is, if you have configured 1000 as the max-flow value for a service set that uses an AMS interface with four active member interfaces, each of the member interfaces can handle 1000 flows each, resulting in an effective max-flow value of 4000.</p> </div>	
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Service Set Limitations on page 753</a></li> </ul>

## message-rate-limit

<b>Syntax</b>	<code>message-rate-limit <i>messages-per-second</i></code>
<b>Hierarchy Level</b>	<pre> interfaces <i>interface-name</i> {   services-options {     cgn-pic;     disable-global-timeout-override;     ignore-errors &lt;alg&gt; &lt;tcp&gt;;     inactivity-non-tcp-timeout <i>seconds</i>;     inactivity-tcp-timeout <i>seconds</i>;     inactivity-timeout <i>seconds</i>;     open-timeout <i>seconds</i>;     session-limit {       maximum <i>number</i>;       rate <i>new-sessions-per-second</i>;     }     session-timeout <i>seconds</i>;     syslog {     }   } }</pre>
<b>Release Information</b>	Statement introduced Junos OS Release 11.1.
<b>Description</b>	Maximum system log messages per second allowed from this interface.
<div>  <p><b>NOTE:</b> The <code>message-rate-limit</code> command can be configured only for physical service interfaces (<code>sp-x/x/x</code>) and not for redundancy services PIC interfaces (<code>rspx</code>).</p> </div>	
<b>Options</b>	<p><b><i>messages-per-second</i></b>—This option configures the maximum number of system log messages per second that can be formatted and sent from the PIC to either the Routing Engine (local) or to an external server (remote). The default rates are 10,000 for the Routing Engine and 200,000 for an external server.</p> <p><b>Range:</b> 0 through 2147483647</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring System Logging for Service Sets on page 754</a></li> </ul>


## nat-options

<b>Syntax</b>	<pre>nat-options {   land-attack-check (ip-only   ip-port);   max-sessions-per-subscriber <i>session-number</i>;   stateful-nat64 {     clear-dont-fragment-bit;   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced with Junos OS Release 12.1. <b>land-attack-check</b> and <b>max-sessions-per-subscriber</b> statements added in 13.3.
<b>Description</b>	Specify parameters for NAT operation.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Service Rules on page 747</a></li> <li>• <i>clear-dont-fragment-bit</i></li> <li>• <i>land-attack-check</i></li> <li>• <i>max-sessions-per-subscriber</i></li> <li>• <i>stateful-nat64</i></li> </ul>


## nat-rules

<b>Syntax</b>	(nat-rules <i>rule-name</i>   nat-rule-sets <i>rule-set-name</i> );
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the Network Address Translation (NAT) rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.
<b>Options</b>	<p><b><i>rule-name</i></b>—Identifier for the collection of terms that constitute this rule.</p> <p><b><i>rule-set-name</i></b>—Identifier for the set of rules to be included.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Service Rules on page 747</a></li> </ul>

## next-hop-service

<b>Syntax</b>	<pre> next-hop-service {   inside-service-interface <i>interface-name.unit-number</i>;   outside-service-interface <i>interface-name.unit-number</i>;   outside-service-interface-type local;   service-interface-pool <i>name</i>; } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p><b>service-interface-pool</b> option added in Junos OS Release 9.3.</p>
<b>Description</b>	Specify interface names or a service interface pool for the forwarding next-hop service set. You cannot specify both a service interface pool and an inside or outside interface.
<b>Options</b>	<p><b>inside-service-interface <i>interface-name.unit-number</i></b>—Name and logical unit number of the service interface associated with the service set applied inside the network.</p> <p><b>outside-service-interface <i>interface-name.unit-number</i></b>—Name and logical unit number of the service interface associated with the service set applied outside the network.</p> <p><b>outside-service-interface-type <i>interface-type</i></b>—Identifies the interface type of the service interface associated with the service set applied outside the network. For inline IP reassembly, set the interface type to local.</p> <p><b>service-interface-pool <i>name</i></b>—Name of the pool of logical interfaces configured at the [edit <a href="#">services service-interface-pools pool pool-name</a>] hierarchy level. You can configure a service interface pool only if the service set has a PGCP rule configured. The service set cannot contain any other type of rule.</p>
<div>  <p><b>NOTE:</b> <b>service-interface-pool</b> is not applicable for IP reassembly configuration on L2TP.</p> </div>	
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li> </ul>

## no-anti-replay (Services Service Set)

<b>Syntax</b>	no-anti-replay;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> service-set <i>service-set-name</i> ipsec-vpn-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	<p>Disable IPsec antireplay service for this service set, which occasionally causes interoperability issues for security associations. This statement is useful for dynamic endpoint tunnels for which you cannot configure the <b>no-anti-reply</b> statement at the [edit <a href="#">services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</a>] hierarchy level.</p> <p>For static IPsec tunnels, this statement disables the antireplay check for all the tunnels within this service set. If antireplay check has to be enabled for a particular tunnel, then set the <b>anti-replay-window-size</b> statement at the [edit <a href="#">services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</a>] hierarchy level.</p>
	<div>  <p><b>NOTE:</b> Setting the anti-replay-window-size and no-anti-replay statements at the [edit <a href="#">services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i> then</a>] hierarchy level overrides the settings specified at the [edit <a href="#">services service-set <i>service-set-name</i> ipsec-vpn-options</a>] hierarchy level.</p> </div>
<b>Usage Guidelines</b>	See or .
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring IPsec Service Sets on page 748</a></li> <li>• <a href="#">Configuring or Disabling IPsec Anti-Replay on page 510</a></li> </ul>

## passive-mode-tunneling

---

<b>Syntax</b>	<code>passive-mode-tunneling;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ipsec-vpn-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Allows tunneling of malformed packets. When this statement is enabled, traffic bypasses the usual active IP checks. The IPsec tunnel is not treated as a next hop and TTL is not decremented. If the packet size exceeds the tunnel MTU value, an ICMP error is not generated.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IPsec Service Sets on page 748</a></li></ul>

## pgcp-rules

---

<b>Syntax</b>	<code>(pgcp-rules <i>rule-name</i>   pgcp-rules-sets <i>rule-set-name</i>);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Specify the Packet Gateway Control Protocol (PGCP) rules or rule set included in this service set. You can configure multiple rules but only one rule set for each service.
<b>Options</b>	<i>rule-name</i> —Identifier for the collection of terms that constitute this rule. <i>rule-set-name</i> —Identifier for the set of rules to be included.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li></ul>

## port (syslog)

---

<b>Syntax</b>	<code>port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> <a href="#">services-options</a> <a href="#">syslog</a> <a href="#">host</a> <i>hostname</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	UDP port for system log messages on the host. The default port is 514.
<b>Options</b>	<i>port-number</i> —Port number for system log messages.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring System Logging for Services Interfaces on page 801</a></li> </ul>

## ptsp-rules

---

<b>Syntax</b>	<code>(ptsp-rules <i>rule-name</i>   ptsp-rules-sets <i>rule-set-name</i>);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">service-set</a> <i>service-set-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the PTSP rules or rule set included in this service set. You can configure multiple rules but only one rule set for each service.
<b>Options</b>	<i>rule-name</i> —Identifier for the collection of terms that constitute this rule. <i>rule-set-name</i> —Identifier for the set of rules to be included.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li> </ul>

## service-interface

---

<b>Syntax</b>	<code>service-interface <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name interface-service</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the name for the adaptive services interface associated with an interface-wide service set.
<b>Options</b>	<i>interface-name</i> —Identifier of the service interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li></ul>

## service-set (Services)

```
Syntax  service-set service-set-name {
        allow-multicast;
        extension-service service-name {
            provider-specific-rules-configuration;
        }
        (ids-rules rule-name | ids-rule-sets rule-set-name);
        interface-service {
            service-interface interface-name;
        }
        ipsec-vpn-options {
            anti-replay-window-size bits;
            clear-dont-fragment-bit;
            ike-access-profile profile-name;
            local-gateway address;
            no-anti-replay;
            passive-mode-tunneling;
            trusted-ca [ ca-profile-names ];
            tunnel-mtu bytes;
        }
        ip-reassembly-rules rule-name;
        (ipsec-vpn-rules rule-name | ipsec-vpn-rule-sets rule-set-name);
        max-flows number;
        max-drop-flows {
            ingress ingress-flows;
            egress egress-flows;
        }
        nat-options {
            land-attack-check (ip-only | ip-port);
            max-sessions-per-subscriber session-number;
            stateful-nat64 {
                clear-dont-fragment-bit;
            }
        }
        (nat-rules rule-name | nat-rule-sets rule-set-name);
        next-hop-service {
            inside-service-interface interface-name.unit-number;
            outside-service-interface interface-name.unit-number;
            outside-service-interface-type local;
            service-interface-pool name;
        }
        (pgcp-rules rule-name | pgcp-rule-sets rule-set-name);
        (ptsp-rules rule-name | ptsp-rule-sets rule-set-name);
        service-set-options {
            bypass-traffic-on-exceeding-flow-limits;
            bypass-traffic-on-pic-failure;
            enable-asymmetric-traffic-processing;
            support-uni-directional-traffic;
        }
        snmp-trap-thresholds {
            flows high high-threshold | low low-threshold;
            nat-address-port high-threshold | low low-threshold;
        }
    }
```

```

}
software-options {
    dslite-ipv6-prefix-length dslite-ipv6-prefix-length;
}
(software-rules rule-name | software-rule-sets rule-set-name);
(stateful-firewall-rules rule-name | stateful-firewall-rule-sets rule-set-name);
syslog {
    host hostname {
        class {
            alg-logs;
            ids-logs;
            nat-logs;
            packet-logs;
            pcp-logs;
            session-logs <open | close>;
            stateful-firewall-logs ;
        }
        services severity-level;
        facility-override facility-name;
        interface-service prefix-value;
    }
}
}

```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced before Junos OS Release 7.4.  
**pgcp-rules** and **pgcp-rule-sets** options added in Junos OS Release 8.4.  
**server-set-options** option added in Junos OS Release 10.1.  
**ptsp-rules** and **ptsp-rule-sets** options added in Junos OS Release 10.2.  
**software-rules** and **clear-rule-sets** options added in Junos OS Release 10.4.  
**software-options** option added in Junos OS Release 14.1.

**Description** Define the service set.

**Options** *service-set-name*—Name of the service set.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
 interface-control—To add this statement to the configuration.

**Related Documentation**

- *Service Set Properties*

## service-set-options

<b>Syntax</b>	<pre>service-set-options {   bypass-traffic-on-exceeding-flow-limits;   bypass-traffic-on-pic-failure;   enable-asymmetric-traffic-processing;   support-uni-directional-traffic;   header-integrity-check }</pre>
<b>Hierarchy Level</b>	[edit services service-set]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1. The <b>enable-asymmetric-traffic-processing</b> and the <b>support-uni-directional-traffic</b> options were added in Release 11.2.
<b>Description</b>	Specify the service set options to apply to a service set.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li> <li>• <a href="#">Configuring APPID Support for Unidirectional Traffic on page 1007</a></li> </ul>

## softwire-options

<b>Syntax</b>	<pre>softwire-options {   dslite-ipv6-prefix-length <i>dslite-ipv6-prefix-length</i> ; }</pre>
<b>Hierarchy Level</b>	[edit services <b>service-set</b> <i>service-set-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Specify the IPv6 prefix length associated with a subscriber's basic broadband bridging device that is subject to a limited number of sessions.
<b>Options</b>	<p><b><i>dslite-ipv6-prefix-length</i></b>—Subnet prefix representing the size of the subnet subject to session limitation.</p> <p><b>Values:</b> 56, 64, 96, 128</p> <p><b>Default:</b> 0—no limitation.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">DS-Lite Per Subnet Limitation Overview</a></li> </ul>

## services

---

See the following sections:

- [services \(Hierarchy\) on page 786](#)
- [services \(System Logging\) on page 787](#)

### services (Hierarchy)

<b>Syntax</b>	<code>services { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the service rules to be applied to traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Service Set Properties</i></li></ul>

## services (System Logging)

<b>Syntax</b>	<code>services severity-level;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name syslog host hostname</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the severity level for system logging messages.
<b>Options</b>	<p><b>severity-level</b>—Assigns a severity level to the facility. Valid entries are:</p> <ul style="list-style-type: none"><li>• <b>alert</b>—Conditions that should be corrected immediately.</li><li>• <b>any</b>—Matches any level.</li><li>• <b>critical</b>—Critical conditions.</li><li>• <b>emergency</b>—Panic conditions.</li><li>• <b>error</b>—Error conditions.</li><li>• <b>info</b>—Informational messages.</li><li>• <b>notice</b>—Conditions that require special handling.</li><li>• <b>warning</b>—Warning messages.</li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Logging for Service Sets on page 754</a></li></ul>

## set-dont-fragment-bit (Services Set)

---

<b>Syntax</b>	set-dont-fragment-bit;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> service-set <i>service-set-name</i> ipsec-vpn-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Configure the do not fragment (DF) bit in only the outer header of the IPsec packet and leave the inner header unmodified for dynamic endpoint tunnels. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. These settings apply for dynamic endpoint tunnels and not for static tunnels, for which you need to include the <b>set-dont-fragment-bit</b> statement at the [edit <a href="#">services ipsec-vpn rule rule-name term term-name then</a> ] hierarchy level to set the DF bit in the outer header of the IPv4 packets that enter the static IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IPsec Service Sets on page 748</a></li><li>• <a href="#">Configuring Actions in IPsec Rules on page 508</a></li></ul>

## stateful-firewall-rules

---

<b>Syntax</b>	(stateful-firewall-rules <i>rule-names</i>   stateful-firewall-rule-sets <i>rule-set-name</i> );
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the stateful firewall rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.
<b>Options</b>	<i>rule-name</i> —Identifier for the collection of terms that make up this rule.  <i>rule-set-name</i> —Identifier for the set of rules to be included.
<b>Required Privilege Level</b>	System—To view this statement in the configuration. System-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Rules on page 747</a></li></ul>

## syslog (Services Service Set)

<b>Syntax</b>	<pre> syslog {   host hostname {     class {       alg-logs;       ids-logs;       nat-logs;       packet-logs;       pcp-logs;       session-logs &lt;open   close&gt;;       stateful-firewall-logs ;     }     services severity-level;     facility-override facility-name;     interface-service prefix-value;   } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Configure generation of system log messages for the service set. The system log information is passed to the kernel for logging in the <code>/var/log</code> directory. These settings override the values defined at the <b>[edit interfaces <i>interface-name</i> services-options]</b> hierarchy level; for more information on configuring those values, see <a href="#">“Configuring System Logging for Services Interfaces” on page 801</a>.</p>
<b>Options</b>	The remaining statements are described separately.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring System Logging for Service Sets on page 754</a></li> </ul>

## tcp-mss

---

<b>Syntax</b>	<code>tcp-mss <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the TCP Maximum Segment Size (MSS) allowed for the service set.
<b>Options</b>	<i>number</i> —MSS value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Set Limitations on page 753</a></li></ul>

## traceoptions (Services Logging)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable       no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace; } </pre>
<b>Hierarchy Level</b>	<p>[edit <a href="#">services adaptive-services-pics</a>], [edit <a href="#">services logging</a>]</p>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4. <b>file</b> option added in Release 8.0.</p>
<b>Description</b>	<p>Configure Adaptive Services or Multiservices PIC tracing operations. The messages are output to <b>/var/log/serviced</b>.</p>
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. All files are placed in the directory <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000 files <b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace everything.</li> <li>• <b>command-queued</b>—Trace command enqueue events.</li> <li>• <b>config</b>—Trace configuration events.</li> <li>• <b>handshake</b>—Trace handshake events.</li> <li>• <b>init</b>—Trace initialization events.</li> <li>• <b>interfaces</b>—Trace interface events.</li> <li>• <b>mib</b>—Trace GGSN SNMP MIB events.</li> <li>• <b>removed-client</b>—Trace client cleanup events.</li> <li>• <b>show</b>—Trace CLI command servicing.</li> </ul> <p><b>match <i>regex</i></b>—(Optional) Match output to a defined regular expression (regex).</p>

**Default:** If you do not include this option, the trace operation output includes all lines relevant to the logged events.

**no-world-readable**—(Optional) Prevent any user from reading the log file.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

**Range:** 10 KB through 1 GB

**Default:** 128 KB

**world-readable**—(Optional) Allow any user to read the log file.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Tracing Services PIC Operations on page 756</a></li></ul>


---

## trusted-ca

---

<b>Syntax</b>	trusted-ca <i>ca-profile-name</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services service-set service-set-name ipsec-vpn-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.5.
<b>Description</b>	Identify one or more trusted IPsec certification authorities.
<b>Options</b>	<b>ca-profile-name</b> —Name of certification authority profile, which is configured at the [edit <a href="#">security pki</a> ] hierarchy level.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration.
	admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring IPsec Service Sets on page 748</a></li></ul>

## tunnel-mtu (Services Service Set)

<b>Syntax</b>	<code>tunnel-mtu bytes;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> service-set <i>service-set-name</i> ipsec-vpn-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	<p>Maximum transmission unit (MTU) size for IPsec tunnels. This statement is useful for dynamic endpoint tunnels for which you cannot configure the <b>tunnel-mtu</b> statement at the [edit <b>services ipsec-vpn rule rule-name term term-name then</b>] hierarchy level.</p> <p>For static IPsec tunnels, this statement sets the tunnel MTU value for all the tunnels within this service set. If you need a specific value for a particular tunnel, then set the <b>tunnel-mtu</b> statement at the [edit <b>services ipsec-vpn rule rule-name term term-name then</b>] hierarchy level.</p>
	<div>  <p><b>NOTE:</b> The <b>tunnel-mtu</b> setting at the [edit <b>services ipsec-vpn rule rule-name term term-name then</b>] hierarchy level overrides the value specified at the [edit <b>services service-set service-set-name ipsec-vpn-options</b>] hierarchy level.</p> </div>
<b>Options</b>	<p><i>bytes</i>—MTU size.</p> <p><b>Default:</b> 1500 bytes</p> <p><b>Range:</b> 256 through 9192 bytes</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">mtu on page 1456</a></li> <li>• <a href="#">Configuring IPsec Service Sets on page 748</a></li> <li>• <a href="#">Specifying the MTU for IPsec Tunnels on page 511</a></li> </ul>



# Service Interface Configuration Guidelines

For the interfaces on a router to function, you must configure them, specifying properties such as the interface location (that is, which slot the Flexible PIC Concentrator [FPC] is installed in and which location on the FPC the Physical Interface Card [PIC] is installed in), the interface type (such as SONET/SDH or Asynchronous Transfer Mode [ATM]), encapsulation, and interface-specific properties. You can configure the interfaces that are currently present in the router, and you can also configure interfaces that are not currently present but that you might add in the future. When a configured interface appears, the Junos OS detects its presence and applies the appropriate configuration to it. For more information on the general configuration of interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

You can configure two different sets of properties at the interface level:

- Properties that apply to an entire Adaptive Services (AS) or Multiservices PIC interface on a global level, including default values for system logging and timeout properties.
- Assignment of service sets and filters to a network interface.

To configure default properties for the adaptive services interface, include the **sp-fpc/pic/port** or **rspnumber** statement at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
(sp-fpc/pic/port | rspnumber) {
  services-options {
    cgn-pic;
    close-timeout
    fragment-limit
    disable-global-timeout-override;
    ignore-errors <alg> <tcp>;
    inactivity-non-tcp-timeout seconds;
    inactivity-tcp-timeout seconds;
    inactivity-timeout seconds;
    open-timeout seconds;
    reassembly-timeout
    session-limit {
      maximum number;
      rate new-sessions-per-second;
    }
    session-timeout seconds;
    syslog {
      host hostname {
```

```

        facility-override facility-name;
        log-prefix prefix-value;
        port port-number;
        services severity-level;
    }
    message-rate-limit messages-per-second;
}
}
}

```

To apply services on network interfaces, include the **unit** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```

unit logical-unit-number {
    clear-dont-fragment-bit;
    encapsulation type;
    family (Interfaces) inet {
        address (Interfaces) address {
            ...
        }
        mtu bytes;
        service {
            input (Interfaces) {
                [ service-set (Interfaces) service-set-name <service-filter filter-name> ];
                post-service-filter filter-name;
            }
            output {
                [ service-set (Interfaces) service-set-name <service-filter filter-name> ];
            }
        }
        service-domain (inside | outside);
    }
}

```

To configure AS or Multiservices PIC redundancy, include the **redundancy-options** statement at the **[edit interfaces *rsp number*]** hierarchy level:

```

rspnumber {
    redundancy-options {
        primary sp-fpc/pic/port;
        secondary sp-fpc/pic/port;
        hot-standby
    }
}

```

To configure an MX-DPC interface to be used exclusively for carrier-grade NAT (CGN) and related services (intrusion detection, stateful firewall, and software), include the **cgn-pic** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level.

This chapter contains the following sections:

- [Services Interface Naming Overview on page 797](#)
- [Configuring the Address and Domain for Services Interfaces on page 798](#)
- [Configuring Default Timeout Settings for Services Interfaces on page 799](#)
- [Configuring System Logging for Services Interfaces on page 801](#)

- [Enabling Fragmentation on GRE Tunnels on page 802](#)
- [Applying Filters and Services to Interfaces on page 803](#)
- [Configuring AS or Multiservices PIC Redundancy on page 806](#)
- [Flow Offloading on page 808](#)
- [Configuring Fragmentation Control for MS-DPC and MS-PIC Service Interfaces. on page 809](#)
- [Examples: Configuring Services Interfaces on page 809](#)

## Services Interface Naming Overview

Each interface has an interface name, which specifies the media type, the slot the FPC is located in, the location on the FPC that the PIC is installed in, and the PIC port. The interface name uniquely identifies an individual network connector in the system. You use the interface name when configuring interfaces and when enabling various functions and properties, such as routing protocols, on individual interfaces. The system uses the interface name when displaying information about the interface, for example, in the **show interfaces** command.

The interface name is represented by a physical part, a logical part, and a channel part in the following format:

**physical<:channel>.logical**

The channel part of the name is optional for all interfaces except channelized DS3, E1, OC12, and STM1 interfaces.

The physical part of an interface name identifies the physical device, which corresponds to a single physical network connector. This part of the interface name has the following format:

**type-fpc/pic/port**

**type** is the media type, which identifies the network device. For service interfaces, it can be one of the following:

- **ams**—Aggregated multiservices (AMS) interface. An AMS interface is a bundle of services interfaces that can function as a single interface. An AMS interface is denoted as **amsN** in the configuration, where **N** is a unique number that identifies an AMS interface (for example, **ams0**). The member interfaces in an AMS interface are identified in the configuration with an **mams-** prefix (for example, **mams-1/2/0**).
- **cp**—Flow collector interface.
- **es**—Encryption interface.
- **gr**—Generic routing encapsulation tunnel interface.
- **gre**—This interface is internally generated and not configurable.
- **ip**—IP-over-IP encapsulation tunnel interface.
- **ipip**—This interface is internally generated and not configurable.

- **ls**—Link services interface.
- **lsq**—Link services intelligent queuing (IQ) interface; also used for voice services.
- **mams**—Member interface in an AMS interface.
- **ml**—Multilink interface.
- **mo**—Monitoring services interface. The logical interface **mo-fpc/pic/port.16383** is an internally generated, nonconfigurable interface for router control traffic.
- **ms**—Multiservices interfaces on multiservices modular interfaces card (MS-MIC) and multiservices modular port concentrators (MS-MPC).
- **mt**—Multicast tunnel interface. This interface is automatically generated, but you can configure properties on it if needed.
- **mtun**—This interface is internally generated and not configurable.
- **rlsq**—Redundancy LSQ interface.
- **rsp**—Redundancy adaptive services interface.
- **si**—Services inline interface, configured on MX3D Series routers only.
- **sp**—Adaptive services interface. The logical interface **sp-fpc/pic/port.16383** is an internally generated, nonconfigurable interface for router control traffic.
- **tap**—This interface is internally generated and not configurable.
- **vp**—Voice over IP (VoIP) interface, configured on J Series Services Routers only.
- **vt**—Virtual loopback tunnel interface.

**Related  
Documentation**

- [Understanding Services PICs on page 3](#)
- [Understanding Aggregated Multiservices Interfaces on page 93](#)
- [Examples: Configuring Services Interfaces on page 809](#)

---

## Configuring the Address and Domain for Services Interfaces

On the AS or Multiservices PIC, you configure a source address for system log messages by including the **address** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet]** hierarchy level:

```
address address {  
  ...  
}
```

Assign an IP address to the interface by configuring the **address** value. The AS or Multiservices PIC generally supports only IP version 4 (IPv4) addresses configured using the **family inet** statement, but IPsec services support IP version 6 (IPv6) addresses as well, configured using the **family inet6** statement.

For information on other addressing properties you can configure that are not specific to service interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

The **service-domain** statement specifies whether the interface is used within the network or to communicate with remote devices. The software uses this setting to determine which default stateful firewall rules to apply, and to determine the default direction for service rules. To configure the domain, include the **service-domain** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level:

```
service-domain (inside | outside);
```

If you are configuring the interface in a next-hop service-set definition, the **service-domain** setting must match the configuration for the **inside-service-interface** and **outside-service-interface** statements; for more information, see “[Configuring Service Sets to be Applied to Services Interfaces](#)” on page 742.

#### Related Documentation

- [Configuring Default Timeout Settings for Services Interfaces](#) on page 799
- [Configuring System Logging for Services Interfaces](#) on page 801
- [Examples: Configuring Services Interfaces](#) on page 809
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\)](#) on page 94

## Configuring Default Timeout Settings for Services Interfaces

You can specify global default settings for certain timers that apply for the entire interface. There are three statements of this type:

- **inactivity-timeout**—Sets the inactivity timeout period for established flows, after which they are no longer valid.
- **open-timeout**—Sets the timeout period for Transmission Control Protocol (TCP) session establishment, for use with SYN-cookie defenses against network intrusion.
- **close-timeout**—Sets the timeout period for Transmission Control Protocol (TCP) session tear-down.

To configure a setting for the inactivity timeout period, include the **inactivity-timeout** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level:

```
[edit interfaces interface-name services-options]
inactivity-timeout seconds;
```

The default value is 30 seconds. The range of possible values is from 4 through 86,400 seconds. Any value you configure in the application protocol definition overrides the value specified here; for more information, see “[Configuring Application Protocol Properties](#)” on page 146.

To configure a setting for the TCP session establishment timeout period, include the **open-timeout** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level:

```
[edit interfaces interface-name services-options]
open-timeout seconds;
```

The default value is 30 seconds. The range of possible values is from 4 through 224 seconds. Any value you configure in the intrusion detection service (IDS) definition overrides the value specified here; for more information, see *Intrusion Detection Properties*.

To configure a setting for the TCP session teardown timeout period, include the **close-timeout** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level:

```
[edit interfaces interface-name services-options]
  close-timeout seconds;
```

The default value is 1 second. The range of possible values is from 2 through 300 seconds.

### Use of Keep-Alive Messages for Greater Control of TCP Inactivity Timeouts

Keep-alive messages are generated automatically to prevent TCP inactivity timeouts. The default number of keep-alive messages is 4. However, you can configure the number of keep-alive messages by entering the **tcp-tickles** statement at the **[edit interfaces *interface-name* service-options]** hierarchy level.

When timeout is generated for a bidirectional TCP flow, keep-alive packets are sent to reset the timer. If number of consecutive keep-alive packets sent in a flow reaches the default or configured limit, the conversation is deleted. There are several possible scenarios, depending on the setting of the **inactivity-timer** and the default or configured maximum number of keep-alive messages.

- If the configured value of keep-alive messages is zero and **inactivity-timeout** is NOT configured (in which case the default timeout value of 30 is used), no keep-alive packets are sent. The conversation is deleted when any flow in the conversation is idle for more than 30 seconds.
- If the configured value of keep-alive messages is zero and the **inactivity-timeout** is configured, no keep-alive packets are sent, and the conversation is deleted when any flow in the conversation is idle for more than the configured timeout value.
- If the default or configured maximum number of keep-alive messages is some positive integer, and any of the flows in a conversation is idle for more than the default or configured value for **inactivity-timeout** keep-alive packets are sent. If hosts do not respond to the configured number of consecutive keep-alive packets, the conversation is deleted. The interval between keep-alive packets will be 1 second. However, if the host sends back an ACK packet, the corresponding flow becomes active, and keep-alive packets are not sent until the flow becomes idle again.

#### Related Documentation

- [Understanding Services PICs on page 3](#)
- [Configuring the Address and Domain for Services Interfaces on page 798](#)
- [Configuring System Logging for Services Interfaces on page 801](#)
- [Applying Filters and Services to Interfaces on page 803](#)
- [Examples: Configuring Services Interfaces on page 809](#)

## Configuring System Logging for Services Interfaces

You specify properties that control how system log messages are generated for the interface as a whole. If you configure different values for the same properties at the **[edit services service-set service-set-name]** hierarchy level, the service-set values override the values configured for the interface. For more information on configuring service-set properties, see [“Configuring System Logging for Service Sets” on page 754](#).

To configure interface-wide default system logging values, include the **syslog** statement at the **[edit interfaces interface-name services-options]** hierarchy level:

```
[edit interfaces interface-name services-options]
syslog {
  host hostname {
    services severity-level;
    facility-override facility-name;
    log-prefix prefix-value;
    port port-number;
  }
}
```

Configure the **host** statement with a hostname or an IP address that specifies the system log target server. The hostname **local** directs system log messages to the Routing Engine. For external system log servers, the hostname must be reachable from the same routing instance to which the initial data packet (that triggered session establishment) is delivered. You can specify only one system logging hostname.

[Table 33 on page 801](#) lists the severity levels that you can specify in configuration statements at the **[edit interfaces interface-name services-options syslog host hostname]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

**Table 33: System Log Message Severity Levels**

Severity Level	Description
<b>any</b>	Includes all severity levels
<b>emergency</b>	System panic or other condition that causes the router to stop functioning
<b>alert</b>	Conditions that require immediate correction, such as a corrupted system database
<b>critical</b>	Critical conditions, such as hard drive errors
<b>error</b>	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
<b>warning</b>	Conditions that warrant monitoring
<b>notice</b>	Conditions that are not errors but might warrant special handling

Table 33: System Log Message Severity Levels (*continued*)

Severity Level	Description
info	Events or nonerror conditions of interest

We recommend setting the system logging severity level to **error** during normal operation. To monitor PIC resource usage, set the level to **warning**. To gather information about an intrusion attack when an intrusion detection system error is detected, set the level to **notice** for a specific interface. To debug a configuration or log Network Address Translation (NAT) functionality, set the level to **info**.

For more information about system log messages, see the *Junos OS System Log Messages Reference*.

To use one particular facility code for all logging to the specified system log host, include the **facility-override** statement at the **[edit interfaces *interface-name* services-options syslog host *hostname*]** hierarchy level:

```
[edit interfaces interface-name services-options]
  facility-override facility-name;
```

The supported facilities include **authorization**, **daemon**, **ftp**, **kernel**, **user**, and **local0** through **local7**.

To specify a text prefix for all logging to this system log host, include the **log-prefix** statement at the **[edit interfaces *interface-name* services-options syslog host *hostname*]** hierarchy level:

```
[edit interfaces interface-name services-options]
  log-prefix prefix-value;
```

#### Related Documentation

- [Understanding Services PICs on page 3](#)
- [Configuring the Address and Domain for Services Interfaces on page 798](#)
- [Configuring Default Timeout Settings for Services Interfaces on page 799](#)
- [Applying Filters and Services to Interfaces on page 803](#)
- [Examples: Configuring Services Interfaces on page 809](#)

## Enabling Fragmentation on GRE Tunnels

To enable fragmentation of IPv4 packets in generic routing encapsulation (GRE) tunnels, include the **clear-dont-fragment-bit** statement and a maximum transmission unit (MTU) setting for the tunnel as part of an existing GRE configuration at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
  gr-fpc/pic/port {
    unit logical-unit-number {
      clear-dont-fragment-bit;
      ...
    }
  }
```

```

family inet {
    mtu 1000;
    ...
}
}

```

This statement clears the Don't Fragment (DF) bit in the packet header, regardless of the packet size. If the packet size exceeds the tunnel MTU value, the packet is fragmented before encapsulation. The maximum MTU size configurable on the AS or Multiservices PIC is 9192 bytes.



**NOTE:** The `clear-dont-fragment-bit` statement is supported only on MX Series routers and all M Series routers except the M320 router.

Fragmentation is enabled only on IPv4 packets being encapsulated in IPv4-based GRE tunnels.



**NOTE:** This configuration is supported only on GRE tunnels on AS or Multiservices interfaces. If you commit `gre-fragmentation` as the encapsulation type on a standard Tunnel PIC interface, the following console log message appears when the PIC comes online:

```
gr-fpc/pic/port: does not support this encapsulation
```

The Packet Forwarding Engine updates the IP identification field in the outer IP header of GRE-encapsulated packets, so that reassembly of the packets is possible after fragmentation. The previous CLI constraint check that required you to configure either the `clear-dont-fragment-bit` statement or a tunnel key with the `allow-fragmentation` statement is no longer enforced.

When you configure the `clear-dont-fragment-bit` statement on an interface with the MPLS protocol family enabled, you must specify an MTU value. This MTU value must not be greater than maximum supported value (9192).

**Related Documentation**

- [Configuring Unicast Tunnels on page 1567](#)

## Applying Filters and Services to Interfaces

When you have defined and grouped the service rules by configuring the service-set definition, you can apply services to one or more interfaces on the router. To associate a defined service set with an interface, include the `service-set` statement with the `input` or `output` statement at the `[edit interfaces interface-name unit logical-unit-number family inet service]` hierarchy level:

```

[edit interfaces interface-name unit logical-unit-number family inet service]
input {
    service-set service-set-name <service-filter filter-name>;
}

```

```

post-service-filter filter-name;
}
output {
  service-set service-set-name <service-filter filter-name>;
}

```



**NOTE:** When you enable services on an interface, reverse-path forwarding is not supported. You cannot configure services on the management interface (fxp0) or the loopback interface (lo0).

You can configure different service sets on the input and output sides of the interface. However, for service sets with bidirectional service rules, you must include the same service set definition in both the **input** and **output** statements. Any service set you include in the **service** statement must be configured with the **interface-service** statement at the **[edit services service-set service-set-name]** hierarchy level; for more information, see [“Configuring Service Sets to be Applied to Services Interfaces” on page 742](#).



**NOTE:** If you configure an interface with an input firewall filter that includes a reject action and with a service set that includes stateful firewall rules, the router executes the input firewall filter before the stateful firewall rules are run on the packet. As a result, when the Packet Forwarding Engine sends an Internet Control Message Protocol (ICMP) error message out through the interface, the stateful firewall rules might drop the packet because it was not seen in the input direction.

Possible workarounds are to include a forwarding-table filter to perform the reject action, because this type of filter is executed after the stateful firewall in the input direction, or to include an output service filter to prevent the locally generated ICMP packets from going to the stateful firewall service.

## Configuring Service Filters

You can optionally include filters associated with each service set to refine the target and additionally process the traffic. If you include the **service-set** statement without a **service-filter** definition, the router software assumes that the match condition is true and selects the service set for processing automatically.

To configure service filters, include the **firewall** statement at the **[edit]** hierarchy level:

```

firewall {
  family inet {
    service-filter filter-name {
      term term-name {
        from {
          match-conditions;
        }
        then {
          action;
          action-modifiers;
        }
      }
    }
  }
}

```

```

    }
  }
}

```



**NOTE:** You must specify `inet` as the address family to configure a service filter.

You configure service filters in a similar way to firewall filters. Service filters have the same match conditions as firewall filters, but the following specific actions:

- **count**—Add the packet to a counter total.
- **log**—Log the packet.
- **port-mirror**—Port-mirror the packet.
- **sample**—Sample the packet.
- **service**—Forward the packet for service processing.
- **skip**—Omit the packet from service processing.

For more information about configuring firewall filters, see the *Routing Policy Feature Guide for Routing Devices*.

You can also include more than one service set definition on each side of the interface. If you include multiple service sets, the router software evaluates them in the order specified in the configuration. It executes the first service set for which it finds a match in the service filter and ignores the subsequent definitions.

An additional statement allows you to specify a filter for processing the traffic after the input service set is executed. To configure this type of filter, include the **post-service-filter** statement at the `[edit interfaces interface-name unit logical-unit-number family inet service input]` hierarchy level:

```
post-service-filter filter-name;
```



**NOTE:** The software performs postservice filtering only when it has selected and executed a service set. If the traffic does not meet the match criteria for any of the configured service sets, the postservice filter is ignored. The **post-service-filter** statement is not supported when the service interface is on an MS-MIC or MS-MPC.

For an example of applying a service set to an interface, see [“Examples: Configuring Services Interfaces” on page 809](#).

For more information on applying filters to interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*. For general information on filters, see the *Routing Policy Feature Guide for Routing Devices*.



**NOTE:** After NAT processing is applied to packets, they are not subject to output service filters. The service filters affect only untranslated traffic.

**Related  
Documentation**

- [Understanding Services PICs on page 3](#)
- [Configuring Service Sets to be Applied to Services Interfaces on page 742](#)
- [Examples: Configuring Services Interfaces on page 809](#)

---

## Configuring AS or Multiservices PIC Redundancy

---

You can configure AS or Multiservices PIC redundancy on M Series and T Series routers, except TX Matrix routers, that have multiple AS or Multiservices PICs. To configure redundancy, you specify a redundancy services PIC (**rsp**) interface in which the primary PIC is active and a secondary PIC is on standby. If the primary PIC fails, the secondary PIC becomes active, and all service processing is transferred to it. If the primary AS or Multiservices PIC is restored, it remains on standby and does not preempt the secondary PIC; you need to manually restore the services to the primary PIC. To determine which PIC is currently active, issue the **show interfaces redundancy** command.

Failover to the secondary PIC occurs under the following conditions:

- The primary PIC, FPC, or Packet Forwarding Engine goes down, resets, or is physically removed from the router.
- The PIC or FPC is taken offline using the **request chassis pic fpc-slot slot-number pic-slot slot-number offline** or **request chassis fpc slot slot-number offline** command. For more information, see the [CLI Explorer](#).
- The driver watchdog timer expires.
- The **request interface switchover** command is issued. For more information, see the [CLI Explorer](#).



**NOTE:** Adaptive Services and Multiservices PICs in Layer-2 mode (running Layer 2 services) are not rebooted when a MAC flow-control situation is detected.



**NOTE:** When you perform a switchover from a primary PIC to a secondary or standby PIC or a revert operation by issuing **request interfaces (revert | switchover)** command for redundancy services PICs (**rsp**), the PIC that was previously the active PIC before the switchover or reversion is automatically rebooted. The reboot of the PIC that was previously active and functioning as the primary PIC does not disrupt traffic forwarding.

The physical interface type **rsp** specifies the pairings between primary and secondary **sp** interfaces to enable redundancy. To configure an AS or Multiservices PIC as the backup, include the **redundancy-options** statement at the **[edit interfaces rspnumber]** hierarchy level:

```
[edit interfaces rspnumber]
redundancy-options {
  primary sp-fpc/pic/port;
  secondary sp-fpc/pic/port;
  hot-standby;
}
```

For the **rsp** interface, *number* can be from 0 through 15.



**NOTE:** You can include a similar redundancy configuration for Link Services IQ (LSQ) PICs at the **[edit interfaces rlsqnumber]** hierarchy level. For more information, see [“Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces” on page 621](#).

The following constraints apply to redundant AS or Multiservices PIC configurations:

- The services supported in redundancy configurations include stateful firewall, NAT, IDS, and IPsec. Services mounted on the AS or Multiservices PIC that use interface types other than **sp**- interfaces, such as tunneling and voice services, are not supported. For information on flow monitoring redundancy, see [“Configuring Services Interface Redundancy with Flow Monitoring” on page 1210](#).



**NOTE:** For IPsec functionality, the router no longer needs to renegotiate security associations (SAs) during warm standby PIC switchover. Instead, the warm standby feature has been made stateful by periodically setting a checkpoint between the working state of the PIC and the Routing Engine, which should lessen the downtime during switchover. If you prefer to retain the earlier behavior, you can include the **clear-ipsec-sas-on-pic-restart** statement at the **[edit services ipsec-vpn]** hierarchy level. If you enable this capability, the router renegotiates the IPsec SAs on warm standby PIC switchover. For more information, see [“Clearing Security Associations” on page 489](#).

- We recommend that you pair the same model type in RSP configurations, such as two ASMs or two AS2 PICs. If you pair unlike models, the two PICs may perform differently.
- You can specify an AS or Multiservices PIC (**sp** interface) as the primary for only one **rsp** interface.
- An **sp** interface can be a secondary for multiple **rsp** interfaces. However, the same **sp** interface cannot be configured as a primary interface in one **rsp** configuration and as a secondary in another configuration.
- When the secondary PIC is active, if another primary PIC that is paired with it in an **rsp** configuration fails, no failover takes place.

- When you configure an AS or Multiservices PIC within a redundant configuration, the **sp** interface cannot have any configured services. Apply the configurations at the **[edit interfaces rspnumber]** hierarchy level, using, for example, the **unit** and **services-options** statements. Exceptions include the **multiservice-options** statement used in flow monitoring configurations, which can be configured separately for the primary and secondary **sp** interfaces, and the **traceoptions** statement.
- All the operational mode commands that apply to **sp** interfaces also apply to **rsp** interfaces. You can issue **show** commands for the **rsp** interface or the primary and secondary **sp** interfaces.
- If a secondary PIC fails while it is in use, the **rsp** interface returns to the “not present” state. If the primary PIC comes up later, service is restored to it.
- For redundant Multiservices (rms-) interfaces, similar to the configuration of other bundle interfaces, the properties of the Multiservices (ms-) member interfaces, such as the logical unit and the address family, are inherited from the underlying rms- interface. If you previously configured the member ms- interface properties separately, and attempt to configure the rms- interface properties by using the relevant statements at the **[edit interfaces rmsnumber]** hierarchy level, an error occurs when you perform a commit check operation. You must configure the properties of interfaces that are part of the rms- interface only by using the statements at the **[edit interfaces rmsnumber]** hierarchy level.

**Related  
Documentation**

- [Understanding Services PICs on page 3](#)
- [Examples: Configuring Services Interfaces on page 809](#)
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\) on page 94](#)

---

## Flow Offloading

The Junos OS enables you to configure flow offloading for PICS on MX Series routers using Modular Port Concentrator (MPCs) with Modular Interface Cards (MICs). Flows are offloaded to Fast Update Filters (FUFs) on the Packet Forwarding Engine. Offloading produces the greatest benefits when applied to long-lasting or high-bandwidth flows

The maximum number of active offloads is 200,000 per PIC. When offloaded flows are deleted, more flows can be offloaded.

To configure flow offloading:

- At the **[edit interfaces interface-name services-options]** hierarchy level, enter the **trio-flow-offload minimum-bytes *minimum-bytes*** statement.

```
user@host# edit services interface-name
[edit services interface-name services-options]
user@host# set trio-flow-offload minimum-bytes minimum-bytes
```

In the following example, flows are offloaded when they consist of no less than 1024 bytes:

```
user@host# edit services ms-0/1/0
```

```
[edit services ms-0/1/0 services-options]
user@host# set trio-flow-offload minimum-bytes 1024
```

Related Documentation

- [trio-flow-offload on page 834](#)

## Configuring Fragmentation Control for MS-DPC and MS-PIC Service Interfaces.

Two configuration options are available to prevent excessive consumption of computational CPU cycles on a services PIC caused by the handling of large numbers of fragmented packets. Such fragment handling can be exploited in DOS attacks. The **fragment-limit** option establishes a maximum number of fragments for a packet. When this number is exceeded, the packet is dropped. The **reassemble-timeout** specifies the maximum time from the receipt of the first and latest fragments in a packet. When the number is exceeded, the packet is dropped.

To configure fragmentation control for MS-DPC and MS-PIC service interfaces:

1. In configuration mode, go to the **[edit interfaces *interface-name* services-options** hierarchy level.

```
edit interfaces interface-name services-options
```

2. Configure the fragment limit.

```
[ edit services interface-name services-options]
set fragment=limit number-of-fragments
```

3. Configure the reassembly timeout.

```
[ edit services interface-name services-options]
set reassembly-timeout number-of-fragments
```

## Examples: Configuring Services Interfaces

Apply the **my-service-set** service set on an interface-wide basis. All traffic that is accepted by **my\_input\_filter** has **my-input-service-set** applied to it. After the service set is applied, additional filtering is done using the **my\_post\_service\_input\_filter** filter.

```
[edit interfaces fe-0/1/0]
unit 0 {
  family inet {
    filter {
      input my_input_filter;
      output my_output_filter;
    }
    service {
      input {
        service-set my-input-service-set;
        post-service-filter my_post_service_input_filter;
      }
      output {
        service-set my-output-service-set;
      }
    }
  }
}
```

```
}  
}
```

Configure two redundancy interfaces, **rsp0** and **rsp1**, and associated services.

```
[edit interfaces]  
rsp0 {  
  redundancy-options {  
    primary sp-0/0/0;  
    secondary sp-1/3/0;  
  }  
  unit 0 {  
    family inet;  
  }  
  unit 30 {  
    family inet;  
    service-domain inside;  
  }  
  unit 31 {  
    family inet;  
    service-domain outside;  
  }  
}  
rsp1 {  
  redundancy-options {  
    primary sp-0/1/0;  
    secondary sp-1/3/0;  
  }  
  unit 0 {  
    family inet;  
  }  
  unit 20 {  
    family inet;  
    service-domain inside;  
  }  
  unit 21 {  
    family inet;  
    service-domain outside;  
  }  
}  
[edit services]  
service-set null-sfw-with-nat {  
  stateful-firewall-rules allow-all;  
  nat-rules rule1;  
  next-hop-service {  
    inside-service-interface rsp0.30;  
    outside-service-interface rsp0.31;  
  }  
}  
[edit routing-instances]  
vpna {  
  interface rsp0.0;  
}
```

**Related Documentation**

- [Understanding Services PICs on page 3](#)

- [Configuring the Address and Domain for Services Interfaces on page 798](#)
- [Configuring Default Timeout Settings for Services Interfaces on page 799](#)
- [Configuring System Logging for Services Interfaces on page 801](#)
- [Applying Filters and Services to Interfaces on page 803](#)
- [Example: Configuring an Aggregated Multiservices Interface \(AMS\) on page 94](#)



## CHAPTER 32

# Summary of Service Interface Configuration Statements

The following sections explain each of the service interface configuration statements. The statements are organized alphabetically.

- [address \(Interfaces\) on page 814](#)
- [cgn-pic on page 815](#)
- [clear-dont-fragment-bit on page 815](#)
- [close-timeout on page 816](#)
- [dial-options on page 817](#)
- [facility-override on page 818](#)
- [family \(Interfaces\) on page 819](#)
- [host \(Interfaces\) on page 820](#)
- [hot-standby on page 820](#)
- [inactivity-timeout on page 821](#)
- [input \(Interfaces\) on page 821](#)
- [interfaces on page 822](#)
- [log-prefix \(Interfaces\) on page 822](#)
- [maximum on page 823](#)
- [open-timeout on page 823](#)
- [output on page 824](#)
- [post-service-filter on page 824](#)
- [primary \(Interfaces\) on page 825](#)
- [rate on page 825](#)
- [redundancy-options on page 826](#)
- [secondary \(Interfaces\) on page 826](#)
- [service on page 827](#)
- [service-domain on page 828](#)
- [service-filter \(Interfaces\) on page 828](#)

- [service-set \(Interfaces\) on page 829](#)
- [services \(Interfaces\) on page 830](#)
- [services-options on page 831](#)
- [session-limit on page 832](#)
- [source-address on page 832](#)
- [syslog \(Interfaces\) on page 833](#)
- [tcp-tickles on page 833](#)
- [trio-flow-offload on page 834](#)
- [unit on page 835](#)

---

## address (Interfaces)

---

<b>Syntax</b>	<code>address address {     ... }</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">unit logical-unit-number family (Interfaces) family</a> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <a href="#">unit logical-unit-number family (Interfaces) family</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the interface address.
<b>Options</b>	<b><i>address</i></b> —Address of the interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li><li>• <a href="#">Configuring the Address and Domain for Services Interfaces on page 798</a></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## cg-n-pic

<b>Syntax</b>	cg-n-pic;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Restrict usage of the service PIC to carrier-grade NAT (CGN) or associated services (intrusion detection, stateful firewall, and software). All memory is available for CGN or related services and can be used for CGN scaling.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card on page 60</a></li> </ul>

## clear-dont-fragment-bit

<b>Syntax</b>	clear-dont-fragment-bit;
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>gr-fpc/pic/port unit logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> <a href="#">interfaces</a> <i>gr-fpc/pic/port unit logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Clear the Don't Fragment (DF) bit on all IP version 4 (IPv4) packets entering the generic routing encapsulation (GRE) tunnel on Adaptive Services (AS) or Multiservices interfaces. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. The statement is supported only on MX Series routers and all M Series routers except the M320 router.</p> <p>When you configure the <b>clear-dont-fragment-bit</b> statement on an interface with the MPLS protocol family enabled, you must specify an MTU value. This MTU value must not be greater than maximum supported value, which is 9192.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Enabling Fragmentation on GRE Tunnels on page 802</a></li> </ul>

## close-timeout

---

<b>Syntax</b>	<code>close-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3.
<b>Description</b>	Configure the timeout period for Transmission Control Protocol (TCP) session tear-down.
<b>Options</b>	<b>seconds</b> —Timeout period. <b>Default:</b> 1 second <b>Range:</b> 2 through 300 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Default Timeout Settings for Services Interfaces on page 799</a></li></ul>

## dial-options

<b>Syntax</b>	<pre>dial-options {   ipsec-interface-id <i>name</i>;   l2tp-interface-id <i>name</i>;   (shared   dedicated); }</pre>
<b>Hierarchy Level</b>	<pre>[edit <a href="#">interfaces</a> sp-fpc/pic/port <a href="#">unit</a> <i>logical-unit-number</i>], [edit interfaces si-fpc/pic/port <a href="#">unit</a> <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> <a href="#">interfaces</a> sp-fpc/pic/port <a href="#">unit</a> <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces si-fpc/pic/port <a href="#">unit</a> <i>logical-unit-number</i>]</pre>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>The <b>[edit ...si-...]</b> hierarchy levels introduced in Junos OS Release 11.4.</p>
<b>Description</b>	Specify the options for configuring logical interfaces for group and user sessions in L2TP or IPsec dynamic endpoint tunneling.
<b>Options</b>	<p><b>dedicated</b>—(LNS on M Series routers and MX Series routers only) Specify that a logical interface can host only one session at a time.</p> <p><b>ipsec-interface-id <i>name</i></b>—(M Series routers only) Interface identifier for group of dynamic peers. This identifier must be replicated at the <b>[edit access profile <i>name</i> client * ike]</b> hierarchy level.</p> <p><b>l2tp-interface-id <i>name</i></b>—Interface identifier that must be replicated at the <b>[edit access profile <i>name</i>]</b> hierarchy level.</p> <p><b>shared</b>—(LNS on M Series routers only) Specify that a logical interface can host multiple (shared) sessions at a time.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Identifier for Logical Interfaces that Provide L2TP Services on page 587</a></li> <li>• <a href="#">Configuring Dynamic Endpoints for IPsec Tunnels on page 512</a></li> <li>• <a href="#">Configuring Options for the LNS Inline Services Logical Interface</a></li> </ul>

## facility-override

---

<b>Syntax</b>	<code>facility-override <i>facility-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> <a href="#">services-options</a> <a href="#">syslog</a> <a href="#">host</a> <i>hostname</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Override the default facility for system log reporting.
<b>Options</b>	<p><i>facility-name</i>—Name of the facility that overrides the default assignment. Valid entries include:</p> <ul style="list-style-type: none"><li><code>authorization</code></li><li><code>daemon</code></li><li><code>ftp</code></li><li><code>kernel</code></li><li><code>local0</code> through <code>local7</code></li><li><code>user</code></li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Logging for Services Interfaces on page 801</a></li></ul>

## family (Interfaces)

<b>Syntax</b>	<pre> family inet {     address address {         ...     }     service {         input {             [ service-set service-set-name &lt;service-filter filter-name&gt; ];             post-service-filter filter-name;         }         output {             [ service-set service-set-name &lt;service-filter filter-name&gt; ];         }     } } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure protocol family information for the logical interface.
<b>Options</b>	<p><b>family</b>—Protocol family. Valid settings for service interfaces include <b>inet</b> (IPv4) and <b>mpls</b>.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li> <li>• <a href="#">Configuring the Address and Domain for Services Interfaces on page 798</a></li> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li> </ul>

## host (Interfaces)

---

<b>Syntax</b>	<pre>host <i>hostname</i> {     <i>services severity-level</i>;     <i>facility-override facility-name</i>;     <i>log-prefix prefix-value</i>;     <i>port port-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces interface-name services-options syslog</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the hostname for the system logging utility.
<b>Options</b>	<p><b>hostname</b>—Name of the system logging utility host machine. This can be the local Routing Engine or an external server address.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying Filters and Services to Interfaces on page 803</a></li></ul>

## hot-standby

---

<b>Syntax</b>	<pre>hot-standby;</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>rlsnumber</i> <a href="#">redundancy-options</a> ], [edit interfaces <i>rlsnumber:number</i> <a href="#">redundancy-options</a> ] [edit interfaces <i>rspnumber</i> <a href="#">redundancy-options</a> ] [edit interfaces <i>rmsnumber</i> <a href="#">redundancy-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	For one-to-one AS, rsp, or rms redundancy configurations, specify that the failure detection and recovery must take place in less than 5 seconds. For FRF.15 (MLFR) and FRF.16 (MFR) configuration, specify the switch over time of 5 seconds and less for FRF.15 and a maximum of 10 seconds for FRF.16.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces on page 621</a></li><li>• <a href="#">Configuring AS or Multiservices PIC Redundancy on page 806</a></li></ul>

## inactivity-timeout

<b>Syntax</b>	<code>inactivity-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the inactivity timeout period for established flows. The timeout value configured in the application protocol definition overrides this value.
<b>Options</b>	<p><b><i>seconds</i></b>—Timeout period.</p> <p><b>Default:</b> 30 seconds</p> <p><b>Range:</b> 4 through 86,400 seconds</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Default Timeout Settings for Services Interfaces on page 799</a></li> </ul>

## input (Interfaces)

<b>Syntax</b>	<pre>input {   <a href="#">service-set</a> <i>service-set-name</i> &lt;<a href="#">service-filter</a> <i>filter-name</i>&gt;;   <a href="#">post-service-filter</a> <i>filter-name</i>; }</pre>
<b>Hierarchy Level</b>	<p>[edit interface <i>interface-name</i> unit <i>logical-unit-number</i> family inet service],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <a href="#">unit</a> <i>logical-unit-number</i> family inet service]</p>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the input service sets and filters to be applied to traffic.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Applying Filters and Services to Interfaces on page 803</a></li> </ul>

## interfaces

---

<b>Syntax</b>	<code>interfaces { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure interfaces on the router.
<b>Default</b>	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## log-prefix (Interfaces)

---

<b>Syntax</b>	<code>log-prefix <i>prefix-value</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> <a href="#">services-options</a> <a href="#">syslog</a> <i>host hostname</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Set the system logging prefix value.
<b>Options</b>	<i>prefix-value</i> —System logging prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Junos OS Services Interfaces Library for Routing Devices</i></li><li>• <a href="#">Configuring System Logging for Services Interfaces on page 801</a></li></ul>

## maximum

---

<b>Syntax</b>	<code>maximum <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options session-limit</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the maximum number of sessions allowed simultaneously.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## open-timeout

---

<b>Syntax</b>	<code>open-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure a timeout period for Transmission Control Protocol (TCP) session establishment.
<b>Options</b>	<b><i>seconds</i></b> —Timeout period. <b>Default:</b> 30 seconds <b>Range:</b> 4 through 224 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Default Timeout Settings for Services Interfaces on page 799</a></li> </ul>

## output

---

<b>Syntax</b>	<pre>output {   [ <b>service-set</b> <i>service-set-name</i> &lt;<b>service-filter</b> <i>filter-name</i>&gt; ]; }</pre>
<b>Hierarchy Level</b>	[edit interface <i>interface-name</i> unit <i>logical-unit-number</i> family inet service], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> family inet service]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the output service sets and filters to be applied to traffic.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying Filters and Services to Interfaces on page 803</a></li></ul>

## post-service-filter

---

<b>Syntax</b>	<pre>post-service-filter <i>filter-name</i>;</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet <b>service input</b> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet <b>service input</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the filter to be applied to traffic after service processing. The filter is applied only if a service set is configured and selected. You can configure a postservice filter on the input side of the interface only.  The <b>post-service-filter</b> statement is not supported when the service interface is on an MS-MIC or MS-MPC.
<b>Options</b>	<b><i>filter-name</i></b> —Identifier for the post-service filter.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying Filters and Services to Interfaces on page 803</a></li></ul>

## primary (Interfaces)

---

<b>Syntax</b>	<code>primary <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> (rsp0   rsp1) <a href="#">redundancy-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the primary adaptive services interface.
<b>Options</b>	<i>interface-name</i> —The identifier for the AS or Multiservices PIC interface, which must be of the form <i>sp-fpc/pic/port</i> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring AS or Multiservices PIC Redundancy on page 806</a></li></ul>

## rate

---

<b>Syntax</b>	<code>rate <i>new-sessions-per-second</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> <a href="#">services-options</a> <a href="#">session-limit</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the maximum number of new sessions allowed per second.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## redundancy-options

---

<b>Syntax</b>	<pre>redundancy-options {     primary sp-fpc/pic/port;     secondary sp-fpc/pic/port;     hot-standby }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> rspnumber] [edit <a href="#">interfaces</a> rmsnumber]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the primary and secondary (backup) adaptive services interfaces.
<b>Options</b>	The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring AS or Multiservices PIC Redundancy</a> ” on page 806.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring AS or Multiservices PIC Redundancy on page 806</a></li></ul>

## secondary (Interfaces)

---

<b>Syntax</b>	<pre>secondary interface-name;</pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> (rsp0   rsp1) <a href="#">redundancy-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the secondary (backup) adaptive services interface.
<b>Options</b>	<i>interface-name</i> —The identifier for the adaptive services interface, which must be of the form <i>sp-fpc/pic/port</i> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring AS or Multiservices PIC Redundancy on page 806</a></li></ul>

## service

---

<b>Syntax</b>	<pre> service {   input {     [ service-set service-set-name &lt;service-filter filter-name&gt; ];     post-service-filter filter-name;   }   output {     [ service-set service-set-name &lt;service-filter filter-name&gt; ];   } } </pre>
<b>Hierarchy Level</b>	<pre> [edit interfaces interface-name unit logical-unit-number family inet], [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet] </pre>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the service sets and filters to be applied to an interface.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Applying Filters and Services to Interfaces on page 803</a></li> </ul>

## service-domain

---

Syntax	service-domain (inside   outside);
Hierarchy Level	[edit <b>interfaces</b> <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet], [edit logical-systems <i>logical-system-name</i> <b>interfaces</b> <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the service interface domain. If you specify this interface using the <b>next-hop-service</b> statement at the [edit <b>services</b> <b>service-set</b> <i>service-set-name</i> ] hierarchy level, the interface domain must match that specified with the <b>inside-service-interface</b> and <b>outside-service-interface</b> statements.
Options	<b>inside</b> —Interface used within the network.  <b>outside</b> —Interface used outside the network.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Address and Domain for Services Interfaces on page 798</a></li></ul>

## service-filter (Interfaces)

---

Syntax	service-filter <i>filter-name</i> ;
Hierarchy Level	[edit <b>interfaces</b> <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet <b>service</b> (input   output) <b>service-set</b> <i>service-set-name</i> ], [edit logical-systems <i>logical-system-name</i> <b>interfaces</b> <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet <b>service</b> (input   output) <b>service-set</b> <i>service-set-name</i> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the filter to be applied to traffic before it is accepted for service processing. Configuration of a service filter is optional; if you include the <b>service-set</b> statement without a <b>service-filter</b> definition, Junos OS assumes the match condition is true and selects the service set for processing automatically.
Options	<b><i>filter-name</i></b> —Identifies the filter to be applied in service processing.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Applying Filters and Services to Interfaces on page 803</a></li><li>• <a href="#">Junos OS Services Interfaces Library for Routing Devices</a></li></ul>

## service-set (Interfaces)

<b>Syntax</b>	<code>service-set <i>service-set-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet <b>service</b> ( <b>input</b>   <b>output</b> )], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet <b>service</b> ( <b>input</b>   <b>output</b> )]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define one or more service sets to be applied to an interface. If you define multiple service sets, the router software evaluates the filters in the order in which they appear in the configuration.
<b>Options</b>	<b><i>service-set-name</i></b> —Identifies the service set.
<b>Required Privilege Level</b>	System—To view this statement in the configuration. System-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Applying Filters and Services to Interfaces on page 803</a></li> </ul>

## services (Interfaces)

---

<b>Syntax</b>	<code>services severity-level;</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> <a href="#">services-options</a> <a href="#">syslog host</a> <i>hostname</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the system logging severity level.
<b>Options</b>	<p><b>severity-level</b>—Assigns a severity level to the facility. Valid entries include:</p> <ul style="list-style-type: none"><li>• <b>alert</b>—Conditions that should be corrected immediately.</li><li>• <b>any</b>—Matches any level.</li><li>• <b>critical</b>—Critical conditions.</li><li>• <b>emergency</b>—Panic conditions.</li><li>• <b>error</b>—Error conditions.</li><li>• <b>info</b>—Informational messages.</li><li>• <b>notice</b>—Conditions that require special handling.</li><li>• <b>warning</b>—Warning messages.</li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Logging for Services Interfaces on page 801</a></li></ul>

## services-options

<b>Syntax</b>	<pre> services-options {   cgn-pic;   close-timeout   fragment-limit   disable-global-timeout-override;   ignore-errors &lt;alg&gt; &lt;tcp&gt;;   inactivity-non-tcp-timeout seconds;   inactivity-tcp-timeout seconds;   inactivity-timeout seconds   open-timeout seconds;   pba-interim-logging-interval seconds;   reassembly-timeout   session-limit {     maximum number;     rate new-sessions-per-second;     cpu-load-threshold percentage;   }   session-timeout seconds;   syslog {     host hostname {       facility-override facility-name;       log-prefix prefix-value;       port port-number;       services severity-level;     }     message-rate-limit messages-per-second;   }   tcp-tickles tcp-tickles;   trio-flow-offload minimum-bytes minimum-bytes; } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the service options to be applied on an interface.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Interface Properties</i>.</li> </ul>


## session-limit

---

Syntax	<pre>session-limit {     <b>maximum</b> <i>number</i>;     <b>rate</b> <i>new-sessions-per-second</i>;     <b>cpu-load-threshold</b> <i>percentage</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> <b>services-options</b> ]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Restrict the maximum number of sessions and the session rate on Multiservices PICs.
Options	<b>session-limit</b> —Restricts the maximum number of sessions and the session rate for Multiservices PICs.  The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## source-address

---

Syntax	<pre>source-address <i>source-address</i></pre>
Hierarchy Level	[edit <b>services</b> <b>service-set</b> <i>service-set-name</i> <b>syslog host</b> <i>hostname</i> ]
Release Information	Statement introduced in Junos OS Release 13.1.
Description	Specify a source address to record in system log messages that are directed to a remote machine specified in the <b>hostname</b> statement.
<div> <b>NOTE:</b> The supported interfaces are ms, rms, and mams interfaces. If you do not specify the interface parameter, the command loops on all supported interfaces.</div>	
Options	<b>source-address</b> —A valid IP address, which is recorded as the message source in messages sent to the remote machines specified in the <b>host hostname</b> statement
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Logging for Service Sets on page 754</a></li><li>• <a href="#">host on page 769</a></li><li>• <a href="#">service-set on page 332</a></li></ul>

## syslog (Interfaces)

<b>Syntax</b>	<pre> syslog {   host hostname {     services severity-level;     facility-override facility-name;     log-prefix prefix-value;     port port-number;   }   message-rate-limit messages-per-second; } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure generation of system log messages for the service set. System log information is passed to the kernel for logging in the <code>/var/log</code> directory. Any values configured in the service set definition override these values.
<b>Options</b>	The remaining statements are described separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring System Logging for Services Interfaces on page 801</a></li> </ul>

## tcp-tickles

<b>Syntax</b>	tcp-tickles <i>tcp-tickles</i> ;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.4.
<b>Description</b>	Define the maximum number of keep-alive messages sent before a TCP session is allowed to timeout.
<b>Options</b>	<i>tcp-tickles</i> —Number of keep-alive messages. <b>Range:</b> 0 through 30 <b>Default:</b> 4
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring Default Timeout Settings for Services Interfaces on page 799</a></li> </ul>

## trio-flow-offload

---

<b>Syntax</b>	trio-flow-offload minimum-bytes <i>minimum-bytes</i> ;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>services-options</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Enable any plug-in or daemon on a PIC to generate a flow offload request to off-load flows to the Packet Forwarding Engine. This command is available on MX Series routers with Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs).
<b>Options</b>	<i>minimum-bytes</i> —The minimum number of bytes that trigger offloading. When this option is omitted, offloading is triggered when both the forward and reverse flows of the session have begun, meaning that at least one packet has flowed in each direction.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Flow Offloading on page 808</a></li></ul>

## unit

<b>Syntax</b>	<pre> unit logical-unit-number {     family inet {         address address {         }         service {             input {                 [ service-set service-set-name &lt;service-filter filter-name&gt; ];                 post-service-filter filter-name;             }             output {                 [ service-set service-set-name &lt;service-filter filter-name&gt; ];             }         }         service-domain (inside   outside);     } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
<b>Options</b>	<p><b>logical-unit-number</b>—Number of the logical unit.</p> <p><b>Range:</b> 0 through 16,384</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li> </ul>



# PGCP Configuration Guidelines for the BGF Feature

To configure the border gateway function (BGF), include the **pgcp** statement at the **[edit services]** hierarchy level:

```
[edit services]
pgcp {
  gateway gateway-name {
    cleanup-timeout seconds;
    gateway-address gateway-address;
    fast-update-filters {
      maximum-terms number-of-terms;
      maximum-fuf-percentage percentage;
    }
    gateway-controller gateway-controller-name {
      controller-address ip-address;
      controller-port port-number;
      interim-ah-scheme {
        algorithm algorithm;
      }
    }
  }
  gateway-port gateway-port;
  graceful-restart {
    maximum-synchronization-mismatches number-of-mismatches;
    seconds;
  }
  data-inactivity-detection {
    inactivity-delay;
    latch-deadlock-delay seconds;
    no-rtcp-check;
    send-notification-on-delay;
    inactivity-duration seconds;
    stop-detection-on-drop;
    report-service-change {
      service-change-type (forced-906) | forced-910;
    }
  }
  h248-options {
    audit-observed-events-returns;
    encoding {
      no-dscp-bit-mirroring;
    }
  }
}
```

```

    use-lower-case
  }
  h248-profile {
    profile-name profile-name;
    profile-version version-number;
  }
  service-change {
    control-association-indications {
      disconnect {
        controller-failure (failover-909 | restart-902);
        reconnect (disconnected-900 | restart-902);
      }
      down {
        administrative (forced-905 | forced-908 | none);
        failure (forced-904 | forced-908 | none);
        graceful (graceful-905 | none);
      }
      up {
        cancel-graceful (none | restart-918);
        failover-cold (failover-920 | restart-901);
        failover-warm (failover-919 | restart-902);
      }
    }
    virtual-interface-indications {
      virtual-interface-down {
        administrative (forced-905 | forced-906 | none);
        graceful (graceful-905 | none);
      }
      virtual-interface-up {
        cancel-graceful (none | restart-918);
        warm (none | restart-900);
      }
    }
    context-indications {
      state-loss (forced-910 | forced-915 | none);
    }
    use-wildcard-response;
  }
}
h248-properties {
  application-data-inactivity-detection {
    ip-flow-stop-detection (regulated-notify | immediate-notify);
  }
  base-root {
    mg-provisional-response-timer-value {
      default milliseconds;
      maximum milliseconds;
      minimum milliseconds;
    }
    mgc-provisional-response-timer-value {
      default milliseconds;
      maximum milliseconds;
      minimum milliseconds;
    }
    mg-originated-pending-limit {
      default number-of-messages;
    }
  }
}

```

```

        maximum number-of-messages;
        minimum number-of-messages;
    }
    mgc-originated-pending-limit {
        default number-of-messages;
        maximum number-of-messages;
        minimum number-of-messages;
    }
    normal-mg-execution-time {
        default milliseconds;
        maximum milliseconds;
        minimum milliseconds;
    }
    normal-mgc-execution-time {
        default milliseconds;
        maximum milliseconds;
        minimum milliseconds;
    }
}
diffserv {
    dscp {
        default (dscp-value | alias | do-not-change);
    }
}
event-timestamp-notification {
    request-timestamp (requested | suppressed | autonomous);
}
hanging-termination-detection {
    timerx seconds;
}
ipsec-transport-security-association security-association-name;
notification-behavior {
    notification-regulation default (once | 0 - 100);
}
platform {
    device interface-name;
    routing-engine;
}
segmentation {
    mg-segmentation-timer {
        default milliseconds;
        maximum milliseconds;
        minimum milliseconds;
    }
    mgc-segmentation-timer {
        default milliseconds;
        maximum milliseconds;
        minimum milliseconds;
    }
}
mg-maximum-pdu-size {
    default bytes;
    maximum bytes;
    minimum bytes;
}
mgc-maximum-pdu-size {
    default bytes;
}

```

```

        maximum bytes;
        minimum bytes;
    }
}
traffic-management {
    max-burst-size {
        default bytes;
        maximum bytes;
        minimum bytes;
        rtcp {
            (fixed-value bytes-per-second | percentage percentage);
        }
    }
    peak-data-rate {
        default bytes-per-second;
        maximum bytes-per-second;
        minimum bytes-per-second;
        rtcp {
            (fixed-value bytes-per-second | percentage percentage);
        }
    }
    sustained-data-rate {
        default bytes-per-second;
        maximum bytes-per-second;
        minimum bytes-per-second;
        rtcp {
            (fixed-value bytes-per-second | percentage percentage);
        }
    }
}
}
inactivity-timer {
    inactivity-timeout {
        detect;
        maximum-inactivity-time {
            default 10-millisecond-units;
            maximum 10-millisecond-units;
            minimum 10-millisecond-units;
        }
    }
}
}
h248-timers {
    initial-average-ack-delay milliseconds;
    maximum-net-propagation-delay milliseconds;
    maximum-waiting-delay milliseconds;
    tmax-retransmission-delay milliseconds;
}
max-concurrent-calls number-of-calls;
monitor {
    media {
        rtcp;
        rtp;
    }
}
}
service-state (in-service | out-of-service-forced | out-of-service-graceful);
session-mirroring {

```

```

    delivery-function delivery-function-name {
        destination-address destination-address;
        destination-port destination-port;
        network-operator-id network-operator-id;
        source-address source-address;
        source-port (Mirrored BGF Packets) source-port;
    }
    disable-session-mirroring;
}
}
rule rule-name {
    gateway gateway-name;
    nat-pool nat-pool-name;
}
rule-set rule-set-name {
    rule rule-name;
}
session-mirroring {
    delivery-function delivery-function-name {
        destination-address destination-address;
        destination-port destination-port;
        network-operator-id network-operator-id;
        source-address source-address;
        source-port (Mirrored BGF Packets) source-port;
    }
    disable-session-mirroring;
}
traceoptions {
    file <filename filename> <files number> <match regex> <size size> <world-readable
    | no-world-readable>;
    flag {
        bgf-core {
            common trace-level;
            default trace-level;
            firewall trace-level;
            gate-logic trace-level;
            pic-broker trace-level;
            policy trace-level;
            statistics trace-level;
        }
        default trace-level;
        h248-stack {
            control-association trace-level;
            default trace-level;
            messages;
            media-gateway trace-level;
        }
        sbc-utils {
            common trace-level;
            configuration trace-level;
            default trace-level;
            device-monitor trace-level;
            ipc trace-level;
            memory-management trace-level;
            messaging trace-level;
            user-interface trace-level;
        }
    }
}

```

```
    }  
  }  
}  
virtual-interface number {  
  nat-pool nat-pool-name;  
  routing-instance instance-name {  
    service-interface interface-name.unit-number;  
  }  
  service-state (in-service | out-of-service-forced | out-of-service-graceful);  
}  
}
```

For information about using the PGCP statements to configure the BGF feature, see the *Session Border Control Solutions Guide Using BGF and IMSG*.

# Summary of PGCP Configuration Statements

The following sections explain each of the PGCP statements, which are used to configure the BGF feature. The statements are organized alphabetically.

- [algorithm on page 849](#)
- [application-data-inactivity-detection on page 849](#)
- [audit-observed-events-returns on page 850](#)
- [base-root on page 851](#)
- [bgf-core on page 852](#)
- [cleanup-timeout on page 855](#)
- [context-indications on page 856](#)
- [control-association-indications on page 857](#)
- [controller-address on page 858](#)
- [controller-failure on page 858](#)
- [controller-port on page 859](#)
- [data-inactivity-detection \(Services PGCP\) on page 859](#)
- [default on page 860](#)
- [delivery-function on page 861](#)
- [destination-address on page 861](#)
- [destination-port on page 862](#)
- [detect on page 862](#)
- [diffserv on page 863](#)
- [disable-session-mirroring on page 863](#)
- [disconnect on page 864](#)
- [down on page 865](#)
- [dscp \(Services PGCP\) on page 866](#)
- [encoding on page 866](#)
- [event-timestamp-notification on page 867](#)

- [failover-cold on page 867](#)
- [failover-warm on page 868](#)
- [failure on page 869](#)
- [fast-update-filters on page 870](#)
- [file \(Services PGCP\) on page 871](#)
- [flag \(Services PGCP\) on page 872](#)
- [gateway \(Services PGCP\) on page 873](#)
- [gateway-address on page 877](#)
- [gateway-controller on page 878](#)
- [gateway-port on page 879](#)
- [graceful-restart on page 881](#)
- [h248-options on page 882](#)
- [h248-profile on page 884](#)
- [h248-properties on page 885](#)
- [h248-stack on page 888](#)
- [h248-timers on page 889](#)
- [hanging-termination-detection on page 889](#)
- [inactivity-delay on page 890](#)
- [inactivity-duration \(Services PGCP\) on page 890](#)
- [inactivity-timeout on page 891](#)
- [inactivity-timer on page 892](#)
- [initial-average-ack-delay on page 892](#)
- [interim-ah-scheme on page 893](#)
- [ip-flow-stop-detection on page 893](#)
- [ipsec-transport-security-association on page 894](#)
- [latch-deadlock-delay on page 894](#)
- [max-concurrent-calls on page 897](#)
- [maximum-fuf-percentage on page 898](#)
- [maximum-inactivity-time on page 899](#)
- [maximum-net-propagation-delay on page 900](#)
- [maximum-synchronization-mismatches on page 900](#)
- [maximum-terms on page 901](#)
- [maximum-waiting-delay on page 901](#)
- [media on page 902](#)
- [mg-maximum-pdu-size on page 903](#)
- [mg-originated-pending-limit on page 904](#)
- [mg-provisional-response-timer-value on page 905](#)

- [mg-segmentation-timer](#) on page 906
- [mgc-maximum-pdu-size](#) on page 907
- [mgc-originated-pending-limit](#) on page 908
- [mgc-provisional-response-timer-value](#) on page 909
- [mgc-segmentation-timer](#) on page 910
- [monitor](#) on page 911
- [network-operator-id](#) on page 911
- [no-dscp-bit-mirroring](#) on page 912
- [no-rtcp-check](#) on page 912
- [normal-mg-execution-time](#) on page 913
- [normal-mgc-execution-time](#) on page 914
- [notification-behavior](#) on page 915
- [notification-rate-limit](#) on page 915
- [notification-regulation](#) on page 916
- [overload-control](#) on page 916
- [platform](#) on page 919
- [profile-name](#) on page 920
- [profile-version](#) on page 920
- [queue-limit-percentage](#) on page 921
- [reconnect](#) on page 922
- [reject-all-commands-threshold](#) on page 922
- [reject-new-calls-threshold](#) on page 923
- [report-service-change](#) on page 923
- [request-timestamp](#) on page 924
- [routing-instance](#) on page 924
- [rtcp](#) on page 925
- [rtp](#) on page 925
- [rule](#) on page 926
- [rule-set](#) on page 926
- [sbc-utils \(Services PGCP\)](#) on page 927
- [segmentation](#) on page 928
- [send-notification-on-delay](#) on page 929
- [service-change](#) on page 930
- [service-change-type](#) on page 931
- [service-interface](#) on page 931
- [services \(PGCP\)](#) on page 933
- [session-mirroring](#) on page 934

- [source-address](#) on page 934
- [source-port \(Mirrored BGP Packets\)](#) on page 935
- [state-loss](#) on page 936
- [stop-detection-on-drop](#) on page 936
- [timerx](#) on page 939
- [tmax-retransmission-delay](#) on page 939
- [traceoptions \(Services PGCP\)](#) on page 940
- [traffic-management](#) on page 941
- [up](#) on page 942
- [use-lower-case](#) on page 942
- [use-wildcard-response](#) on page 943
- [virtual-interface](#) on page 944
- [virtual-interface-down](#) on page 945
- [virtual-interface-indications](#) on page 946
- [virtual-interface-up](#) on page 946
- [warm](#) on page 947

## administrative

See the following sections:

- [administrative \(Control Association\) on page 847](#)
- [administrative \(Virtual Interface\) on page 848](#)

### administrative (Control Association)

<b>Syntax</b>	<code>administrative (forced-905   forced-908   none);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services (PGCP)</a> <code>pgcp gateway (Services PGCP) gateway-name h248-options service-change control-association-indications down]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of an administrative operation.
<b>Default</b>	If you do not specify an option, the virtual BGF includes FO/905 ( <b>forced-905</b> ).
<b>Options</b>	<p><b>forced-905</b>—Termination is being taken out of service. The virtual BGF is transitioning to Out-of-Service because of an administrative operation.</p> <p><b>forced-908</b>—Termination is being taken out of service. The virtual BGF is transitioning to Out-of-Service because of an administrative operation or error.</p> <p><b>none</b>—The virtual BGF does not send a ServiceChange command to the gateway controller.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## administrative (Virtual Interface)

<b>Syntax</b>	administrative (forced-905   forced-906   none);
<b>Hierarchy Level</b>	[edit <a href="#">services (PGCP)</a> <a href="#">pgcp gateway (Services PGCP)</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change virtual-interface-indications</a> <a href="#">virtual-interface-down</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller when a virtual interface changes to Out-of-Service because of an administrative operation.
<b>Default</b>	If you do not specify an option, the virtual BGF includes FO/905 ( <b>forced-905</b> ).
<b>Options</b>	<p><b>forced-905</b>—Termination is being taken out of service. The virtual interface is transitioning to Out-of-Service because of an administrative operation.</p> <p><b>forced-906</b>—Loss of lower-layer connectivity. The virtual interface is transitioning to Out-of-Service because of a loss of Layer 2 connectivity caused by the logical or physical interface being administratively disabled.</p> <p><b>none</b>—Virtual BGF does not send a ServiceChange command.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## algorithm

<b>Syntax</b>	<code>algorithm <i>algorithm</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">gateway-controller</a> <i>gateway-controller-name</i> <a href="#">interim-ah-scheme</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Specify the algorithm for the interim AH scheme. Once you set the algorithm for the interim AH scheme, to disable the interim AH scheme, you need to remove the algorithm and restart the PGCP service.
<b>Options</b>	<i>algorithm</i> —Algorithm used for the interim AH scheme. HMAC null is currently the only algorithm supported. <b>Values:</b> hmac-null
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## application-data-inactivity-detection

<b>Syntax</b>	<code>application-data-inactivity {     <a href="#">ip-flow-stop-detection</a> (regulated-notify   immediate-notify); }</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Activate or deactivate regulated notification of media inactivity events.
<b>Options</b>	The statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring H.248 Notification Behavior to Prevent Excessive Media Inactivity Notifications in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## audit-observed-events-returns

---

<b>Syntax</b>	audit-observed-events-returns;
<b>Hierarchy Level</b>	[edit services pgcp gateway <i>gateway-name</i> <b>h248-options</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Enable a history of media inactivity events to be viewed by the gateway controller.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring H.248 Notification Behavior to Prevent Excessive Media Inactivity Notifications in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## base-root

```
Syntax  base-root {
        mg-provisional-response-timer-value {
            default milliseconds;
            maximum milliseconds;
            minimum milliseconds;
        }
        mgc-provisional-response-timer-value {
            default milliseconds;
            maximum milliseconds;
            minimum milliseconds;
        }
        mg-originated-pending-limit {
            default number-of-messages;
            maximum number-of-messages;
            minimum number-of-messages;
        }
        mgc-originated-pending-limit {
            default number-of-messages;
            maximum number-of-messages;
            minimum number-of-messages;
        }
        normal-mg-execution-time {
            default milliseconds;
            maximum milliseconds;
            minimum milliseconds;
        }
        normal-mgc-execution-time {
            default milliseconds;
            maximum milliseconds;
            minimum milliseconds;
        }
    }
```

**Hierarchy Level** [edit [services pgcp gateway gateway-name h248-properties](#)]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Configure default values for properties in the base root package defined in Annex E of *Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005*.

**Options** The statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring H.248 Base Root Properties in Session Border Control Solutions Guide Using BGF and IMSG*

## bgf-core

---

Syntax	<pre>bgf-core {   default <i>trace-level</i>;   firewall <i>trace-level</i>;   gate-logic <i>trace-level</i>;   pic-broker <i>trace-level</i>;   policy <i>trace-level</i>;   statistics <i>trace-level</i>; }</pre>
Hierarchy Level	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">traceoptions</a> <a href="#">flag</a> ]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Configure trace-level options for the BGF core component of the virtual BGF.
Options	<p><b>default <i>trace-level</i></b>—Default trace level for all <b>bgf-core</b> messages.</p> <p><b>firewall <i>trace-level</i></b>—Trace level for the <b>firewall</b> subcomponent, which controls firewall filters, connections, and all relevant firewall activities.</p> <p><b>gate-logic <i>trace-level</i></b>—Trace level for the <b>gate-logic</b> subcomponent, which controls gate common logic, gate lookup, and gate manager activities.</p> <p><b>pic-broker <i>trace-level</i></b>—Trace level for the <b>pic-broker</b> subcomponent, which controls gates on the PIC.</p> <p><b>policy <i>trace-level</i></b>—Trace level for the <b>policy</b> subcomponent, which controls media function and socket policy.</p> <p><b>statistics <i>trace-level</i></b>—Trace level for the <b>statistics</b> subcomponent, which provides pgcpd statistics.</p> <p><b><i>trace-level</i></b>—Trace-level options are related to the severity of the event being traced. When you choose a trace level, messages at that level and higher levels are captured. Enter one of the following trace levels as the <b><i>trace-level</i></b>:</p> <ul style="list-style-type: none"><li>• <b>debug</b>—Logging of all code flow of control.</li><li>• <b>trace</b>—Logging of program trace START and EXIT macros.</li><li>• <b>info</b>—Summary logs for normal operations, such as the policy decisions made for a call.</li><li>• <b>warning</b>—Failure recovery or failure of an external entity.</li><li>• <b>error</b>—Failure with a short-term effect, such as failed processing of a single call.</li></ul>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

- Related Documentation**
- *Session Border Control Solutions Guide Using BGF and IMSG*

## cancel-graceful

---

See the following sections:

- [cancel-graceful \(Control Association\) on page 854](#)
- [cancel-graceful \(Virtual Interface\) on page 855](#)

### cancel-graceful (Control Association)

<b>Syntax</b>	cancel-graceful (none   restart-918);
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-options service-change control-association-indications up</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from the Draining state to the Forwarding state.
<b>Default</b>	If you do not specify an option, the virtual BGF does not send a ServiceChange command.
<b>Options</b>	<b>none</b> —The virtual BGF does not send a ServiceChange command to the gateway controller.  <b>restart-918</b> —The control association has returned to the Forwarding state.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## cancel-graceful (Virtual Interface)

<b>Syntax</b>	cancel-graceful (none   restart-918);
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-options service-change virtual-interface-indications virtual-interface-up</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the virtual interface transitions from In-Service to Out-of-Service-Graceful.
<b>Default</b>	If you do not specify an option, the virtual BGF does not send a ServiceChange command.
<b>Options</b>	<p><b>none</b>—Virtual BGF does not send a ServiceChange command.</p> <p><b>restart-918</b>—Cancel graceful. The virtual interface has entered the Draining state.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## cleanup-timeout

<b>Syntax</b>	cleanup-timeout <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure the number of seconds before the virtual BGF automatically deletes all gates following a disconnection from the gateway controller.
<b>Options</b>	<p><b>seconds</b>—Interval before inactivity detection starts.</p> <p><b>Range:</b> 0 through 65,535 seconds</p> <p><b>Default:</b> 3600 seconds</p>
<b>Required Privilege Level</b>	<p>interface-level—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring a Virtual BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## context-indications

---

<b>Syntax</b>	context-indications { state-loss (forced-910   forced-915   none); }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller when the gates of a context no longer provide their configured services. When the virtual BGF sends a Service-Interruption message, both terminations in the context become Out-of-Service.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Contexts</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## control-association-indications

<b>Syntax</b>	<pre>control-association-indications {   disconnect {     controller-failure (failover-909   restart-902);     reconnect (disconnected-900   restart-902);   }   down {     administrative (forced-905   forced-908   none);     failure (forced-904   forced-908   none);     graceful (graceful-905   none);   }   up {     cancel-graceful (none   restart-918);     failover-cold (failover-920   restart-901);     failover-warm (failover-919   restart-902);   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of the control association changes.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## controller-address

---

<b>Syntax</b>	<code>controller-address ip-address;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">gateway-controller</a> <i>gateway-controller-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure an IP address for the gateway controller.
<b>Options</b>	<i>ip-address</i> —IP address of the gateway controller.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring a Gateway Controller in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## controller-failure

---

<b>Syntax</b>	<code>controller-failure (failover-909   restart-902);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> <a href="#">control-association-indications</a> <a href="#">disconnect</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected.
<b>Default</b>	If you do not specify an option, the virtual BGF includes RS/902 ( <b>restart-902</b> ).
<b>Options</b>	<b>failover-909</b> —Gateway controller impending failure. The virtual BGF is reregistering with a new gateway controller following a disconnection of the virtual BGF and gateway controller.  <b>restart-902</b> —Warm boot. The virtual BGF is attempting to reregister with existing states after a gateway controller failure.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## controller-port

<b>Syntax</b>	<code>controller-port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">gateway-controller</a> <i>gateway-controller-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure the port number of the gateway controller listening port. The virtual BGF sends H.248 messages to this port.
<b>Options</b>	<i>port-number</i> —Port number of the gateway controller.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## data-inactivity-detection (Services PGCP)

<b>Syntax</b>	<pre>data-inactivity-detection {   <a href="#">inactivity-delay</a> <i>seconds</i>;   <a href="#">inactivity-duration</a> <i>seconds</i>;   <a href="#">latch-deadlock-delay</a> <i>seconds</i>;   <a href="#">no-rtcp-check</a>;   <a href="#">send-notification-on-delay</a>;   <a href="#">stop-detection-on-drop</a>;   <a href="#">report-service-change</a> {     <a href="#">service-change-type</a> (<i>forced-906</i>)   <i>forced-910</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure data inactivity detection to detect latch deadlocks or other media inactivity on a gate.
<b>Options</b>	The statements are described separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring Latch Deadlock and Media Inactivity Detection in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## default

---

<b>Syntax</b>	<code>default <i>trace-level</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> traceoptions <a href="#">flag</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure the minimum trace level for all selected PGCP trace options. This option overrides individual trace options that are set at a lower level.
<b>Default</b>	<b>warning</b>
<b>Options</b>	<b><i>trace-level</i></b> —Enter one of the following trace levels as the <b><i>trace-level</i></b> : <ul style="list-style-type: none"><li>• <b>debug</b>—Logging of all code flow of control.</li><li>• <b>trace</b>—Logging of program trace START and EXIT macros.</li><li>• <b>info</b>—Summary logs for normal operations, such as the policy decisions made for a call.</li><li>• <b>warning</b>—Failure recovery or failure of an external entity.</li><li>• <b>error</b>—Failure with a short-term effect, such as failed processing of a single call.</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Tracing BGF Operations in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## delivery-function

<b>Syntax</b>	<code>delivery-function <i>delivery-function-name</i> {     <i>destination-address</i> <i>destination-address</i>;     <i>destination-port</i> <i>destination-port</i>;     <i>network-operator-id</i> <i>network-operator-id</i>;     <i>source-address</i> <i>source-address</i>;     <i>source-port</i> (Mirrored BGF Packets) <i>source-port</i>; }</code>
<b>Hierarchy Level</b>	[edit services pgcp <a href="#">session-mirroring</a> ], [edit services pgcp <a href="#">gateway (Services PGCP)</a> <i>gateway-name</i> <a href="#">session-mirroring</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2
<b>Description</b>	Configure the delivery function that receives the session mirroring information. You can configure only one delivery function.
<b>Options</b>	<b><i>delivery-function-name</i></b> —Name of the delivery function that receives the session mirroring information.
<b>Required Privilege Level</b>	pgcp-session-mirroring—To view this statement in the configuration. pgcp-session-mirroring-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Setting Up Session Mirroring in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## destination-address

<b>Syntax</b>	<code>destination-address <i>destination-address</i>;</code>
<b>Hierarchy Level</b>	[edit services pgcp <a href="#">session-mirroring</a> <a href="#">delivery-function</a> <i>delivery-function-name</i> ], [edit services pgcp <a href="#">gateway (Services PGCP)</a> <i>gateway-name</i> <a href="#">session-mirroring</a> <a href="#">delivery-function</a> <i>delivery-function-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the address of the delivery function server to which the BGF sends session-mirroring information.
<b>Options</b>	<b><i>destination-address</i></b> —Address of the server to which the BGF sends session-mirroring information.
<b>Required Privilege Level</b>	pgcp-session-mirroring—To view this statement in the configuration. pgcp-session-mirroring-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Setting Up Session Mirroring in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## destination-port

---

<b>Syntax</b>	<code>destination-port destination-port;</code>
<b>Hierarchy Level</b>	[edit services pgcp <a href="#">session-mirroring</a> <a href="#">delivery-function</a> <i>delivery-function-name</i> ], [edit services pgcp <a href="#">gateway</a> ( <a href="#">Services PGCP</a> ) <i>gateway-name</i> <a href="#">session-mirroring</a> <a href="#">delivery-function</a> <i>delivery-function-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the port on the delivery function server that receives session-mirroring information.
<b>Options</b>	<b><i>destination-port</i></b> —Port on the delivery function server that receives session-mirroring information. <b>Range:</b> 1 through 65,535
<b>Required Privilege Level</b>	pgcp-session-mirroring—To view this statement in the configuration. pgcp-session-mirroring-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Setting Up Session Mirroring in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## detect

---

<b>Syntax</b>	<code>detect;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">inactivity-timer</a> <a href="#">inactivity-timeout</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify whether the BGF detects inactivity timeout events received from the BGF by default.
<b>Default</b>	The BGF does not detect inactivity timeout events by default.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Detecting Gateway Controller Failures in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## diffserv

<b>Syntax</b>	<pre>diffserv {   dscp {     default (dscp-value   alias   do-not-change);   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-properties</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Configure default values for properties in the Differentiated Services (DiffServ) package defined in Annex A.2 of <i>Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005</i> .
<b>Options</b>	Statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## disable-session-mirroring

<b>Syntax</b>	disable-session-mirroring;
<b>Hierarchy Level</b>	[edit services pgcp <a href="#">session-mirroring</a> ], [edit services pgcp <a href="#">gateway (Services PGCP) gateway-name session-mirroring</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Disable or enable session mirroring on the BGF. To disable session mirroring, enter <b>set disable-session-mirroring</b> . To enable session mirroring, enter <b>delete disable-session-mirroring</b> .
<b>Required Privilege Level</b>	pgcp-session-mirroring—To view this statement in the configuration. pgcp-session-mirroring-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Disabling Session Mirroring in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## disconnect

---

<b>Syntax</b>	<pre>disconnect {   controller-failure (failover-909   restart-902)   reconnect (disconnected-900   restart-902) }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-options service-change control-association-indications</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in Service Change Commands</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## down

---

<b>Syntax</b>	<pre>down {   administrative (forced-905   forced-908   none);   failure (forced-904   forced-908   none);   graceful (graceful-905   none); }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-options service-change control-association-indications</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Unregistration Messages in ServiceChange commands that it sends to the gateway controller when a control association transitions to Out-of-Service because of a failure. The failure can be the result of a services PIC or DPC, or because the services PIC or DPC was powered off or removed.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li> <li>• <i>Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## dscp (Services PGCP)

---

Syntax	<pre>dscp {     default (<i>dscp-value</i>   <i>alias</i>   do-not-change); }</pre>
Hierarchy Level	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">diffserv</a> ]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure default values for DSCP marking that the virtual BGF uses for outgoing traffic when the DSCP value is not already defined by the gateway controller.
Default	The default DSCP value that the virtual BGF uses is zero (0x00).
Options	<p><b>dscp-value</b>—Specify a string of eight bits or a 1-byte hexadecimal value using the format: 0xXX. Currently, only six bits are used by the packet.</p> <p><b>alias</b>—Specify a standard DSCP name. The standard name is translated to an 8-bit string with the two least significant bits (LSBs) as zeros; for example, <b>EF=10111000</b>.</p> <p><b>do-not-change</b>—Specify that no DSCP action be performed on the PIC or DPC. The egress value on the gate is the same as the ingress DSCP value.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Quality of Service for VoIP Traffic Overview</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## encoding

---

Syntax	<pre>encoding {     <a href="#">no-dscp-bit-mirroring</a>;     <a href="#">use-lower-case</a>; }</pre>
Hierarchy Level	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> ]
Release Information	Statement introduced in Junos OS Release 9.3. <b>use-lower-case</b> option introduced in Release 9.5.
Description	Change encoding defaults.
Options	The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## event-timestamp-notification

<b>Syntax</b>	event-timestamp-notification { request-timestamp (requested   suppressed   autonomous); }
<b>Hierarchy Level</b>	[edit services pgcp gateway <i>gateway-name</i> h248-properties]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Enable or disable access by the gateway controller to timestamp information for media inactivity event notifications.
<b>Options</b>	The statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Quality of Service for VoIP Traffic Overview</i> in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li> </ul>

## failover-cold

<b>Syntax</b>	failover-cold (failover-920   restart-901);
<b>Hierarchy Level</b>	[edit services pgcp gateway <i>gateway-name</i> h248-options service-change control-association-indications up]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Registration ServiceChange commands when it attempts to register with a new gateway controller following a cold failover.
<b>Default</b>	If you do not specify an option, the virtual BGF includes RS/901 ( <b>restart-901</b> ).
<b>Options</b>	<p><b>failover-920</b>—Cold failover. The virtual BGF is registering following a graceful Routing Engine switchover. The installed state is reset.</p> <p><b>restart-901</b>—Cold boot. The virtual BGF is transitioning to In-Service. The previously installed state is not retained.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the Method and Reason in ServiceChange Commands for Control Associations</i> in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li> </ul>

## failover-warm

---

<b>Syntax</b>	failover-warm (failover-919   restart-902);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> <a href="#">control-association-indications</a> up]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Registration ServiceChange commands when it attempts to register with a new gateway controller following a warm failover.
<b>Default</b>	If you do not specify an option, the virtual BGF includes RS/902 ( <b>restart-902</b> ).
<b>Options</b>	<p><b>failover-919</b>—Gateway controller impending failure. The virtual BGF is registering with a new gateway controller after the virtual BGF and the gateway controller were disconnected.</p> <p><b>restart-902</b>—Warm boot. The virtual BGF is transitioning to In-Service. The previously installed state is retained.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## failure

<b>Syntax</b>	failure (forced-904   forced-908   none);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> <a href="#">control-association-indications</a> down]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Unregistration or Notification Messages in ServiceChange commands when a control association transitions to Out-of-Service.
<b>Default</b>	If you do not specify an option, the virtual BGF sends ServiceChange command forced-904 to the gateway controller.
<b>Options</b>	<p><b>forced-904</b>—Termination malfunctioning. The virtual BGF is transitioning to Out-of-Service because of a failure.</p> <p><b>forced-908</b>—The virtual BGF is transitioning to Out-of-Service due to administrator action or a failure.</p> <p><b>none</b>—The virtual BGF does not send a ServiceChange command to the gateway controller.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## fast-update-filters

---

<b>Syntax</b>	<pre>fast-update-filters {     maximum-terms <i>number-of-terms</i>;     maximum-fuf-percentage <i>percentage-of-gates</i>; }</pre>
<b>Hierarchy Level</b>	[edit services pgcp gateway <i>gateway-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Limit the number of FUF terms installed on the Packet Forwarding Engine for a virtual BGF to improve performance when the software is collecting statistics on packets that are dropped because they exceed the rate limits set in fast update filters (FUFs).
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Improving Performance While Collecting Gate Statistics in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## file (Services PGCP)

<b>Syntax</b>	file <filename> <files files> <match regular-expression> <size maximum-file-size> <world-readable   no-world-readable>;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp traceoptions]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure the trace file for tracing BGF components.
<b>Options</b>	<p><b>filename filename</b>—Name of the file to which the tracing messages are written.  <b>Default:</b> bsg_trace</p> <p><b>files number-of-files</b>—Number of trace files. The tracing mechanism can rotate between any given number of files, allowing for trace message inspection without interfering with the normal work of the application.  <b>Default:</b> 3</p> <p><b>match regular-expression</b>—Regular expression to match with incoming messages. Messages that do not match the regular expression are not written to the trace file.</p> <p><b>size maximum-trace-file-size</b>—Size parameter (in bytes) to trigger rotation of files. The trace mechanism rotates files based on the current file size. When the size is bigger than the maximum configured size, the files are rotated.  <b>Default:</b> 1048576</p> <p><b>world-readable   no-world-readable</b>—Allow all users to use the log file or disallow all users from using the log file.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Tracing BGF Operations in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li> </ul>

## flag (Services PGCP)

---

**Syntax**

```
flag {  
  default trace-level;  
  bgf-core {  
    default trace-level;  
    firewall trace-level;  
    gate-logic trace-level;  
    pic-broker trace-level;  
    policy trace-level;  
    statistics trace-level;  
  }  
  h248-stack {  
    default trace-level;  
    messages;  
    control-association trace-level;  
    media-gateway trace-level;  
  }  
  sbc-utils {  
    common trace-level;  
    configuration trace-level;  
    device-monitor trace-level;  
    ipc trace-level;  
    memory-management trace-level;  
    message trace-level;  
    minimum trace-level;  
    user-interface trace-level;  
  }  
}
```

**Hierarchy Level** [edit [services](#) pgcp [gateway](#) *gateway-name* [traceoptions](#)]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Configure trace options for components of the BGF.

**Options** The options are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Tracing BGF Operations in Session Border Control Solutions Guide Using BGF and IMSG*

## gateway (Services PGCP)

```
Syntax  pgcp {
    gateway gateway-name {
        cleanup-timeout seconds;
        gateway-address gateway-address;
        gateway-controller gateway-controller-name {
            local-controller | remote-controller;
            controller-address ip-address;
            controller-port port-number;
            interim-ah-scheme {
                algorithm algorithm;
            }
        }
    }
    gateway-port gateway-port;
    service-state (in-service | out-of-service-forced | out-of-service-graceful);
    graceful-restart {
        maximum-synchronization-mismatches number-of-mismatches;
        seconds;
    }
    data-inactivity-detection {
        inactivity-delay seconds;
        latch-deadlock-delay seconds;
        send-notification-on-delay;
        inactivity-duration seconds;
        no-rtcp-check;
        stop-detection-on-drop;
        report-service-change {
            service-change-type (forced-906 | forced-910);
        }
    }
    h248-properties {
        application-data-inactivity-detection {
            ip-flow-stop-detection (regulated-notify | immediate-notify);
        }
        base-root {
            mg-provisional-response-timer-value {
                default milliseconds;
                maximum milliseconds;
                minimum milliseconds;
            }
            mgc-provisional-response-timer-value {
                default milliseconds;
                maximum milliseconds;
                minimum milliseconds;
            }
            mg-originated-pending-limit {
                default number-of-messages;
                maximum number-of-messages;
                minimum number-of-messages;
            }
            mgc-originated-pending-limit {
                default number-of-messages;
                maximum number-of-messages;
            }
        }
    }
}
```

```

        minimum number-of-messages;
    }
    normal-mg-execution-time {
        default milliseconds;
        maximum milliseconds;
        minimum milliseconds;
    }
    normal-mgc-execution-time {
        default milliseconds;
        maximum milliseconds;
        minimum milliseconds;
    }
}
diffserv {
    dscp {
        default (dscp-value | alias | do-not-change);
    }
}
event-timestamp-notification {
    request-timestamp (requested | suppressed | autonomous);
}
hanging-termination-detection {
    timerx seconds;
}
ipsec-transport-security-association security-association-name;
notification-behavior {
    notification-regulation default (once | 0-100);
}
platform {
    device interface-name;
    routing-engine;
}
segmentation {
    mg-segmentation-timer {
        default milliseconds;
        maximum milliseconds;
        minimum milliseconds;
    }
    mgc-segmentation-timer {
        default milliseconds;
        maximum milliseconds;
        minimum milliseconds;
    }
    mg-maximum-pdu-size {
        default bytes;
        maximum bytes;
        minimum bytes;
    }
    mgc-maximum-pdu-size {
        default bytes;
        maximum bytes;
        minimum bytes;
    }
}
traffic-management {
    max-burst-size {

```

```

    default bytes-per-second;
    maximum bytes-per-second;
    minimum bytes-per-second;
    rtcp {
        (fixed-value bytes-per-second | percentage percentage);
    }
}
peak-data-rate {
    default bytes-per-second;
    maximum bytes-per-second;
    minimum bytes-per-second;
    rtcp {
        (fixed-value bytes-per-second | percentage percentage);
    }
    rtcp-include;
}
sustained-data-rate (All Streams) {
    default bytes-per-second;
    maximum bytes-per-second;
    minimum bytes-per-second;
    rtcp {
        (fixed-value bytes-per-second | percentage percentage);
    }
    rtcp-include;
}
}
inactivity-timer {
    inactivity-timeout {
        detect;
        maximum-inactivity-time {
            default 10-millisecond-units;
            maximum 10-millisecond-units;
            minimum 10-millisecond-units;
        }
    }
}
}
h248-options {
    accept-emergency-calls-while-graceful;
    audit-observed-events-returns;
    encoding {
        no-dscp-bit-mirroring;
        use-lower-case;
    }
    h248-profile {
        profile-name profile-name;
        profile-version version-number;
    }
    implicit tcp-latch;
    implicit-tcp-source-filter;
    service-change {
        control-association-indications {
            disconnect {
                controller-failure (failover-909 | restart-902);
                reconnect (disconnected-900 | restart-902);
            }
        }
    }
}

```

```

    down {
        administrative (forced-905 | forced-908 | none);
        failure (forced-904 | forced-908 | none);
        graceful (graceful-905 | none );
    }
    up {
        cancel-graceful (none | restart-918);
        failover-cold (failover-920 | restart-901);
        failover-warm (failover-919 | restart-902);
    }
}
virtual-interface-indications {
    virtual-interface-down {
        administrative (forced-905 | forced-906 | none);
        graceful (graceful-905 | none);
    }
    virtual-interface-up {
        cancel-graceful (Virtual Interface) (none | restart-918);
        warm (none | restart-900);
    }
}
context-indications {
    state-loss (forced-910 | forced-915 | none);
}
use-wildcard-response;
}
}
h248-timers {
    initial-average-ack-delay milliseconds;
    maximum-net-propagation-delay milliseconds;
    maximum-waiting-delay milliseconds;
    tmax-retransmission-delay milliseconds;
}
max-concurrent-calls number-of-calls;
monitor {
    media {
        rtcp;
        rtp;
    }
}
service-state (in-service | out-of-service-forced | out-of-service-graceful);
session-mirroring {
    delivery-function delivery-function-name {
        destination-address destination-address;
        destination-port destination-port;
        network-operator-id network-operator-id;
        source-address source-address;
        source-port (Mirrored BGF Packets) source-port;
    }
    disable-session-mirroring;
}
}
}

```

Hierarchy Level [edit [services](#) pgcp]

<b>Release Information</b>	<p>Statement introduced in Junos OS Release 8.4.</p> <p><b>graceful-restart</b> option introduced in Junos OS Release 8.5.</p> <p><b>h248-options</b> option introduced in Junos OS Release 8.5.</p> <p><b>h248-properties</b> option introduced in Junos OS Release 8.5.</p> <p><b>monitor</b> option introduced in Junos OS Release 9.0.</p> <p><b>session-mirroring</b> option introduced in Junos OS Release 9.2.</p> <p><b>data-inactivity-detection</b> option introduced in Junos OS Release 9.3.</p> <p><b>overload-control</b> option introduced in Junos OS Release 9.3.</p> <p><b>platform</b> option introduced in Junos OS Release 9.6.</p> <p><b>h248-profile</b> option introduced in Junos OS Release 10.0.</p> <p><b>ipsec-transport-security-association</b> option introduced in Junos OS Release 10.0.</p>
<b>Description</b>	Configure a virtual BGF on the router.
<b>Options</b>	<p><b>gateway-name</b>—Identifier of the virtual BGF. You can configure an IP address as the gateway name. However, the IP address is not used in the operation of the virtual BGF.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>BGF VoIP Solution Overview</i> in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li> <li>• <i>BGF VoIP Solution Architecture</i> in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li> <li>• <i>Configuring a Virtual BGF</i> in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li> </ul>

## gateway-address

<b>Syntax</b>	<code>gateway-address gateway-address;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> gateway-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure the IP address of the virtual BGF.
<b>Options</b>	<b>gateway-address</b> —IP address of the virtual BGF that you are configuring on the router.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring a Virtual BGF</i> in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li> </ul>

## gateway-controller

---

Syntax	<pre>gateway-controller <i>gateway-controller-name</i> {     local-controller   remote-controller;     &lt;controller-address <i>ip-address</i>&gt;;     &lt;controller-port <i>port-number</i>&gt;;     interim-ah-scheme {         algorithm <i>algorithm</i>;     } }</pre>
Hierarchy Level	[edit <b>services</b> pgcp <b>gateway</b> <i>gateway-name</i> ]
Release Information	Statement introduced in Junos OS Release 8.4. <b>local-controller</b> option introduced in Junos OS Release 9.4. <b>remote-controller</b> option introduced in Junos OS Release 9.4.
Description	Configure a gateway controller.
Options	<p><b>gateway-controller-name</b>—Name of the gateway controller or BSG. You can configure an IP address as the gateway controller name. However, the IP address is not used for the connection to the gateway controller.</p> <p><b>local-controller   remote-controller</b>—Type of gateway controller.</p> <ul style="list-style-type: none"><li>• <b>remote-controller</b>. Configure the gateway controller as a remote controller if you are using an external gateway controller. You must specify <b>controller-address</b> and <b>controller-port</b>.</li><li>• <b>local-controller</b>. Configure the gateway controller as a local controller if you are using a border signaling gateway (BSG).</li></ul> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring a Virtual BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## gateway-port

---

<b>Syntax</b>	<code>gateway-port gateway-port;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> gateway-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure a port number for the virtual BGF.
<b>Options</b>	<b>gateway-port</b> —Port number of the virtual BGF that you are configuring on the router. <b>Range:</b> 0 through 65,535 <b>Default:</b> 2944
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring a Virtual BGF</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## graceful

---

See the following sections:

- [graceful \(Control Association\) on page 880](#)
- [graceful \(Virtual Interface\) on page 881](#)

### graceful (Control Association)

<b>Syntax</b>	<code>graceful (graceful-905   none);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-options service-change control-association-indications down</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the control association transitions from In-Service to Out-of-Service-Graceful.
<b>Default</b>	If you do not specify an option, the virtual BGF does not send a ServiceChange command.
<b>Options</b>	<b>graceful-905</b> —Termination is being taken out of service. The control association has entered the Draining state.  <b>none</b> —The virtual BGF does not send a ServiceChange command to the gateway controller.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## graceful (Virtual Interface)

<b>Syntax</b>	<code>graceful (graceful-905   none);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-options service-change virtual-interface-indications virtual-interface-down</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Notification ServiceChange commands that it sends to the gateway controller when the virtual interface transitions from In-Service to Out-of-Service-Graceful.
<b>Default</b>	If you do not specify an option, the virtual BGF does not send a ServiceChange command.
<b>Options</b>	<p><b>graceful-905</b>—Termination is being taken out of service. The interface has entered the Draining state.</p> <p><b>none</b>—Virtual BGF does not send a ServiceChange command.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## graceful-restart

<b>Syntax</b>	<code>graceful-restart {     <a href="#">maximum-synchronization-mismatches seconds</a>;     seconds; }</code>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Configure graceful restart properties that are used during synchronization between the pgcpd process and the Multiservices PIC or DPC.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring Synchronization Properties in Case of Routing Engine Failure in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## h248-options

```
Syntax  h248-options {
        accept-emergency-calls-while-graceful;
        audit-observed-events-returns;
        encoding {
            no-dscp-bit-mirroring;
            use-lower-case;
        }
        h248-profile {
            profile-name profile-name;
            profile-version version-number;
        }
        implicit-tcp-latch;
        implicit-tcp-source-filter;
        service-change {
            control-association-indications {
                disconnect {
                    controller-failure (failover-909 | restart-902);
                    reconnect (disconnected-900 | restart-902);
                }
                down {
                    administrative (forced-905 | forced-908 | none);
                    failure (forced-904 | forced-908 | none);
                    graceful (graceful-905 | none);
                }
                up {
                    cancel-graceful (none | restart-918);
                    failover-cold (failover-920 | restart-901);
                    failover-warm (failover-919 | restart-902);
                }
            }
            virtual-interface-indications {
                virtual-interface-down {
                    administrative (forced-905 | forced-906 | none);
                    graceful (graceful-905 | none);
                }
                virtual-interface-up {
                    cancel-graceful (none | restart-918);
                    warm (none | restart-900);
                }
            }
            context-indications {
                state-loss (forced-910 | forced-915 | none);
            }
            use-wildcard-response;
        }
    }
```

**Hierarchy Level** [edit [services](#) [pgcp](#) [gateway](#) *gateway-name*]

**Release Information** Statement introduced in Junos OS Release 8.5.  
**accept-emergency-calls-while-graceful** option introduced in Junos OS Release 10.2.  
**audit-observed-events-returns** option introduced in Junos OS Release 9.3.

	<p><b>encoding</b> option introduced in Junos OS Release 9.3.</p> <p><b>service-change</b> option introduced in Junos OS Release 9.3.</p> <p><b>use-lower-case</b> option introduced in Junos OS Release 9.5.</p> <p><b>h248-profile</b> option introduced in Junos OS Release 10.0.</p> <p><b>-latch</b> option introduced in Junos OS Release 10.4.</p> <p><b>-source-filter</b> option introduced in Junos OS Release 10.4.</p>
<b>Description</b>	Configure options that affect virtual BGF H.248 behavior.
<b>Options</b>	<p><b>accept-emergency-calls-while-graceful</b>—Accept emergency calls when the BGF is in a draining state due to a graceful shutdown.</p> <p><b>-latch</b>—If explicit latching has been applied (using <code>ipnapt/latch</code>) on either gate of a gate pair, implicit latching is <i>not</i> applied. If explicit latching has not been applied on either gate, latching is applied to both gates of the gate pair. When either of the gates latches, latching is automatically disabled on the other gate.</p> <p><b>-source-filter</b>—<b>-source-filter</b>—Applies source address (but not source port) filtering on incoming packets, using the current remote destination address if explicit source filtering has not been applied by use of <code>gm/saf</code> or <code>ipnapt/latch</code>.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p><b>interface</b>—To view this statement in the configuration.</p> <p><b>interface-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Preventing Excessive Media Inactivity Notifications in Session Border Control Solutions Guide Using BGF and IMSG</i></li> <li>• <i>Enabling Wildcards for ServiceChange Notifications in Session Border Control Solutions Guide Using BGF and IMSG</i></li> <li>• <i>Configuring Implicit Latching for TCP Gates in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## h248-profile

---

<b>Syntax</b>	<pre>h248-profile {   profile-name profile-name;   profile-version version-number; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services (PGCP)</a> pgcp <a href="#">gateway (Services PGCP)</a> gateway-name <a href="#">h248-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Configure the profile that the BGF declares in the initial registration ServiceChange request. The profile is declared according to the H.248 standard. That is, profile-name/profile-version. For example, ETSI_BGF/1.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the H.248 Profile in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## h248-properties

```
Syntax h248-properties {
  application-data-inactivity-detection {
    ip-flow-stop-detection (regulated-notify | immediate-notify)
  }
  base-root {
    mg-provisional-response-timer-value {
      default milliseconds;
      maximum milliseconds;
      minimum milliseconds;
    }
    mgc-provisional-response-timer-value {
      default milliseconds;
      maximum milliseconds;
      minimum milliseconds;
    }
    mg-originated-pending-limit {
      default number-of-messages;
      maximum number-of-messages;
      minimum number-of-messages;
    }
    mgc-originated-pending-limit {
      default number-of-messages;
      maximum number-of-messages;
      minimum number-of-messages;
    }
    normal-mg-execution-time {
      default milliseconds;
      maximum milliseconds;
      minimum milliseconds;
    }
    normal-mgc-execution-time {
      default milliseconds;
      maximum milliseconds;
      minimum milliseconds;
    }
  }
  diffserv {
    dscp {
      default (dscp-value | alias | do-not-change);
    }
  }
  event-timestamp-notification {
    request-timestamp (requested | suppressed | autonomous)
  }
  hanging-termination-detection {
    timerx seconds;
  }
  segmentation {
    mg-segmentation-timer {
      default milliseconds;
      maximum milliseconds;
      minimum milliseconds;
    }
  }
}
```

```

}
mgc-segmentation-timer {
    default milliseconds;
    maximum milliseconds;
    minimum milliseconds;
}
mg-maximum-pdu-size {
    default bytes;
    maximum bytes;
    minimum bytes;
}
mgc-maximum-pdu-size {
    default bytes;
    maximum bytes;
    minimum bytes;
}
}
traffic-management {
    max-burst-size {
        default bytes-per-second;
        maximum bytes-per-second;
        minimum bytes-per-second;
        rtcp {
            (fixed-value bytes-per-second | percentage percentage);
        }
    }
    peak-data-rate {
        default bytes-per-second;
        maximum bytes-per-second;
        minimum bytes-per-second;
        rtcp {
            (fixed-value bytes-per-second | percentage percentage);
        }
    }
    sustained-data-rate (All Streams) {
        default bytes-per-second;
        maximum bytes-per-second;
        minimum bytes-per-second;
        rtcp {
            (fixed-value bytes-per-second | percentage percentage);
        }
        rtcp-include;
    }
    inactivity-timer {
        inactivity-timeout {
            detect;
            maximum-inactivity-time {
                default 10-millisecond-units;
                maximum 10-millisecond-units;
                minimum 10-millisecond-units;
            }
        }
    }
}
}

```

<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> gateway-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. <b>diffserv</b> option introduced in Junos OS Release 9.0. <b>inactivity-timer</b> option introduced in Junos OS Release 9.2. <b>traffic-management</b> option introduced in Junos OS Release 9.2. <b>application-data-inactivity-detection</b> option introduced in Junos OS Release 9.3. <b>event-timestamp-notification</b> option introduced in Junos OS Release 9.3.
<b>Description</b>	Configure default values for H.248 properties.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Rate Limiting for the BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li><li>• <i>Configuring H.248 Base Root Properties in Session Border Control Solutions Guide Using BGF and IMSG</i></li><li>• <i>Configuring H.248 Segmentation Properties in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## h248-stack

---

Syntax	<pre>h248-stack {     default <i>trace-level</i>;     messages <i>trace-level</i>;     control-association <i>trace-level</i>;     media-gateway <i>trace-level</i>; }</pre>
Hierarchy Level	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">traceoptions</a> <a href="#">flag</a> ]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Configure trace-level options for the H.248 stack component of the virtual BGF.
Options	<p><b>default <i>trace-level</i></b>—Default trace level for all <b>h248-stack</b> messages.</p> <p><b>messages</b>—When this option is set, H.248 messages are written to the log file.</p> <p><b>control-association <i>trace-level</i></b>—Trace level for traces relevant to the H.248 control association.</p> <p><b>media-gateway <i>trace-level</i></b>—Trace level for libpgcp.</p> <p><b><i>trace-level</i></b>—Trace-level options are related to the severity of the event being traced. When you choose a trace level, messages at that level and higher levels are captured. Enter one of the following trace levels as the <b><i>trace-level</i></b>:</p> <ul style="list-style-type: none"><li>• <b>debug</b>—Logging of all code flow of control.</li><li>• <b>trace</b>—Logging of program trace START and EXIT macros.</li><li>• <b>info</b>—Summary logs for normal operations, such as the policy decisions made for a call.</li><li>• <b>warning</b>—Failure recovery or failure of an external entity.</li><li>• <b>error</b>—Failure with a short-term effect, such as failed processing of a single call.</li></ul>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><li>• <i>Tracing BGF Operations in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## h248-timers

<b>Syntax</b>	h248-timers { initial-average-ack-delay <i>milliseconds</i> ; maximum-net-propagation-delay <i>milliseconds</i> ; maximum-waiting-delay <i>milliseconds</i> ; tmax-retransmission-delay <i>milliseconds</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure H.248 timers for the PGCP connection.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## hanging-termination-detection

<b>Syntax</b>	hanging-termination-detection { timerx <i>seconds</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable and configure hanging termination detection.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Tracing BGF Operations in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## inactivity-delay

---

<b>Syntax</b>	<code>inactivity-delay seconds;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name data-inactivity-detection</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the time after which the virtual BGF begins checking for data packets on terminations that do not include a latch event.
<b>Options</b>	<b>seconds</b> —Time interval before checking for media inactivity. <b>Range:</b> 0 through 3600 <b>Default:</b> 5
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Latch Deadlock and Media Inactivity Detection in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## inactivity-duration (Services PGCP)

---

<b>Syntax</b>	<code>inactivity-duration seconds;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name data-inactivity-detection</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the time interval that determines inactivity. When the virtual BGF determines that the time since the last packet was received exceeds this duration, the virtual BGF generates an inactivity notification or service change request. The duration timer is the same for terminations with latch events and for terminations without latch events.
<b>Options</b>	<b>seconds</b> —Time during which no packets are received. <b>Range:</b> 5 through 86400 <b>Default:</b> 30
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Latch Deadlock and Media Inactivity Detection in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## inactivity-timeout

<b>Syntax</b>	<pre> inactivity-timeout {   detect;   maximum-inactivity-time {     default 10-millisecond-units;     maximum 10-millisecond-units;     minimum 10-millisecond-units;   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">inactivity-timer</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the inactivity timeout event. The inactivity timeout event is used to detect that the inactivity timer has expired.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Detecting Gateway Controller Failures in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## inactivity-timer

---

<b>Syntax</b>	<pre>inactivity-timer {   inactivity-timeout {     detect;     maximum-inactivity-time {       default 10-millisecond-units;       maximum 10-millisecond-units;       minimum 10-millisecond-units;     }   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-properties</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the inactivity timer package, which allows the BGF to use message inactivity to detect that its active gateway controller has failed.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Detecting Gateway Controller Failures in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## initial-average-ack-delay

---

<b>Syntax</b>	<pre>initial-average-ack-delay milliseconds;</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-timers</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure the value of the average acknowledgment delay (AAD) that the virtual BGF uses before the first AAD is measured. The AAD is explained in Annex D of <i>Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005</i> .
<b>Options</b>	<b>milliseconds</b> —Assumed initial average delay. <b>Range:</b> 0 through 65,535 <b>Default:</b> 4000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## interim-ah-scheme

<b>Syntax</b>	interim-ah-scheme { algorithm hmac-null; }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">gateway-controller</a> <i>gateway-controller-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Set up the BGF to use the interim AH scheme.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Example: Using the BGF to Provide VoIP Solutions in a Next-Generation Network in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## ip-flow-stop-detection

<b>Syntax</b>	ip-flow-stop-detection (regulated-notify   immediate-notify);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">application-data-inactivity-detection</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure regulated or non-regulated (immediate) notification of media inactivity events.
<b>Options</b>	<p><b>regulated-notify</b>—Activate regulated notification of media inactivity events.</p> <p><b>immediate-notify</b>—Activate non-regulated notification of media inactivity events.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring H.248 Notification Behavior to Prevent Excessive Media Inactivity Notifications in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## ipsec-transport-security-association

---

<b>Syntax</b>	<code>ipsec-transport-security-association <i>security-association-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services (PGCP)</a> <code>pgcp</code> <a href="#">gateway (Services PGCP)</a> <code>gateway-name</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify the IPsec security association to be used for this virtual BGF.
<b>Options</b>	<b><i>security-association-name</i></b> —Name of the IPsec security association to be used for this virtual BGF. This is a security association that you configured at the [edit <b>services ipsec</b> ] hierarchy level.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Security for BGF Overview</i> in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li><li>• <i>Configuring IPsec to Protect H.248 Messages in Transport Mode</i> in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li></ul>

## latch-deadlock-delay

---

<b>Syntax</b>	<code>latch-deadlock-delay <i>seconds</i></code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <code>pgcp</code> <a href="#">gateway</a> <code>gateway-name</code> <a href="#">data-inactivity-detection</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the time after which the virtual BGF begins checking for data packets on terminations that include a latch event.
<b>Options</b>	<b><i>seconds</i></b> —Time interval before checking for data packets. <b>Range:</b> 0 through 3600
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Latch Deadlock and Media Inactivity Detection</i> in <i>Session Border Control Solutions Guide Using BGF and IMS</i></li></ul>

## max-burst-size

See the following sections:

- [max-burst-size \(All Streams\)](#) on page 895
- [max-burst-size \(RTCP Streams\)](#) on page 896


### max-burst-size (All Streams)

<b>Syntax</b>	<pre>max-burst-size {   default <i>bytes-per-second</i>;   maximum <i>bytes-per-second</i>;   minimum <i>bytes-per-second</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-properties traffic-management</a> ]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.2.</p> <p><b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.</p>
<b>Description</b>	Configure the maximum burst size for gate streams of any protocol, including RTP.
<b>Default</b>	<p>The virtual BGF uses the default value of 1000 bytes if the Policy command in H.248 messages in ON and both of the following apply:</p> <ul style="list-style-type: none"> <li>• The maximum burst size is not set in the H.248 message.</li> <li>• There is no CLI configuration for maximum burst size.</li> </ul>
<b>Options</b>	<p><b>default <i>bytes-per-second</i></b>—Default maximum burst size.  <b>Range:</b> 20 through 4,294,967,295</p> <p><b>maximum <i>bytes-per-second</i></b>—Maximum burst size.  <b>Range:</b> 20 through 4,294,967,295</p> <p><b>minimum <i>bytes-per-second</i></b>—Minimum maximum burst size.  <b>Range:</b> 20 through 4,294,967,295</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Rate Limiting for the BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## max-burst-size (RTCP Streams)

Syntax	<pre>max-burst-size {   rtcp {     (fixed-value <i>bytes</i>   percentage <i>percentage</i>);   } }</pre>
Hierarchy Level	[edit <a href="#">services (PGCP)</a> <a href="#">pgcp gateway (Services PGCP)</a> <i>gateway-name</i> <a href="#">h248-properties traffic-management</a> ]
Release Information	Statement introduced in Junos OS Release 9.2. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
Description	Configure the maximum burst size for for RTP/RTCP gate streams. You can configure this rate as a fixed value or as a percentage of the RTP gate's rate.
Default	The virtual BGF uses the default value of 100 percent of the RTP gate's maximum burst size if the Policy command in H.248 messages in ON and both of the following apply: <ul style="list-style-type: none"><li>• The maximum burst size is not set in the H.248 message.</li><li>• There is no CLI configuration for maximum burst size.</li></ul>
Options	<b>fixed-value</b> —Value entered is a fixed number of bytes per second.  <b><i>bytes-per-second</i></b> —maximum burst size. <b>Range:</b> 20 through 4,294,967,295  <b>percentage</b> —Value entered is a percentage of the RTP gate's rate.  <b><i>percentage</i></b> —Maximum burst size as a percentage of the RTP gate's rate. <b>Range:</b> 1 through 1000
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring Rate Limiting for the BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## max-concurrent-calls

<b>Syntax</b>	<code>max-concurrent-calls <i>number-of-calls</i>;</code>
<b>Hierarchy Level</b>	[edit services pgcp <b>gateway</b> <i>gateway-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	<p>Configure the maximum number of concurrent calls on the virtual BGF. If you configure multiple virtual BGFs for one service PIC or DPC, you can use this statement to achieve a fair distribution of resources between the virtual BGFs. For example, the Multiservices 500 PIC is capable of 10,000 concurrent calls, and you can divide this number between its associated virtual BGFs.</p> <p>You can overbook concurrent calls to avoid resource idleness. The configured total of all virtual BGF maximum concurrent calls can be greater than the PIC or DPC limit. For example, bgf-1 and bgf-2 are connected to single PIC. If you configure 6000 maximum concurrent calls on bgf-1 and 8000 on bgf-2, bgf-1 can open up to 6000 concurrent calls, and bgf-2 can open up to 8000 concurrent calls. However, when the total number of calls reaches 10,000, neither of the virtual BGFs will be able to open a new context.</p> <p>If the resources on the PIC are exhausted and no more calls are allowed, the virtual BGF sends an H.248 error message to the gateway controller in response to new call requests.</p>
	<div>  <p><b>NOTE:</b> You must take the virtual BGF out of service before changing <code>max-concurrent-calls</code> and restart the pgcpd process after returning the virtual BGF to service.</p> </div>
<b>Options</b>	<p><i>number-of-calls</i>—Maximum number of concurrent calls on the virtual BGF.</p> <p><b>Range:</b> 0 through 10,000</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Virtual BGF in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## maximum-fuf-percentage

---

<b>Syntax</b>	maximum-fuf-percentage <i>percentage</i>
<b>Hierarchy Level</b>	[edit services pgcp gateway <i>gateway-name</i> fast-update-filters]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Along with the <b>maximum-terms</b> statement, limit the number of FUF terms installed on the Packet Forwarding Engine for a virtual BGF. This limit is the maximum value of the <b>maximum-terms</b> and <b>maximum-fuf-percentage</b> statements.
<b>Options</b>	<b>percentage</b> —Maximum percentage of gates with FUF filters relative to all gates currently installed for the virtual BGF. <b>Range:</b> 0 through 100 <b>Default:</b> 10
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Improving Performance While Collecting Gate Statistics in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## maximum-inactivity-time

<b>Syntax</b>	<pre>maximum-inactivity-time {     default 10-millisecond-units;     maximum 10-millisecond-units;     minimum 10-millisecond-units; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-properties inactivity-timer inactivity-timeout</a> ]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.2.</p> <p><b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.</p>
<b>Description</b>	<p>Specify default, maximum, and minimum values for the maximum inactivity time. The default value is used if the gateway controller requests that the BGF detect the inactivity timeout event, but the gateway controller does not set a value for the maximum inactivity time. The maximum and minimum values are used to set limits for the maximum inactivity time set by the gateway controller. The BGF issues an error message if the value received from the gateway controller violates the configured minimum or maximum. If the BGF does not receive a message from the gateway controller before the maximum inactivity time expires, it sends a Notify message to the gateway controller. This timer resets each time the BGF receives a message from the gateway controller.</p>
<b>Options</b>	<p><b>default 10-millisecond-units</b>—Default value for the maximum inactivity time.  <b>Range:</b> 100 through 65,535 (10-millisecond units)  <b>Default:</b> 12,000</p> <p><b>maximum 10-millisecond-units</b>—Maximum value for the maximum inactivity time.  <b>Range:</b> 100 through 65,535 (10-millisecond units)  <b>Default:</b> 12,000</p> <p><b>minimum 10-millisecond-units</b>—Minimum value for the maximum inactivity time.  <b>Range:</b> 100 through 65,535 (10-millisecond units)  <b>Default:</b> 12,000</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Detecting Gateway Controller Failures in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## maximum-net-propagation-delay

---

<b>Syntax</b>	maximum-net-propagation-delay <i>milliseconds</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> gateway-name h248-timers]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure the assumed maximum network propagation delay time. This value is used to calculate the LONG-TIMER as explained in Annex D of <i>Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005</i> .
<b>Options</b>	<b>milliseconds</b> —Duration of the maximum network propagation delay time. <b>Range:</b> 0 through 65,535 milliseconds <b>Default:</b> 40,000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## maximum-synchronization-mismatches

---

<b>Syntax</b>	maximum-synchronization-mismatches <i>number-of-mismatches</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> gateway-name graceful-restart]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Configure the maximum number of mismatches allowed during the synchronization procedure between the pgcpd process and the PIC or DPC. If the number of mismatches exceeds this number, the pgcpd process clears the state of the PIC or DPC and the state of the pgcpd process.
<b>Options</b>	<b>number-of-mismatches</b> —Maximum number of mismatches allowed during the synchronization procedure with the PIC or DPC. <b>Range:</b> 0 through 3000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Synchronization Properties in Case of Routing Engine Failure in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## maximum-terms

<b>Syntax</b>	<code>maximum-terms</code> <i>number-of-terms</i>
<b>Hierarchy Level</b>	[edit services pgcp gateway <i>gateway-name</i> <a href="#">fast-update-filters</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Along with the <b>maximum-fuf-percentage</b> statement, limit the number of FUF terms installed on the Packet Forwarding Engine for a virtual BGF. This limit is the maximum value of the <b>maximum-terms</b> and <b>maximum-fuf-percentage</b> statements.
<b>Options</b>	<i>number-of-terms</i> —Maximum number of FUF terms installed for the virtual BGF. <b>Range:</b> 0 through 20000 <b>Default:</b> 20000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Improving Performance While Collecting Gate Statistics in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## maximum-waiting-delay

<b>Syntax</b>	<code>maximum-waiting-delay</code> <i>milliseconds</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-timers</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Define a maximum waiting delay (MWD) value. When the virtual BGF loses its connection to a gateway controller, it attempts to reconnect to the gateway controller. If the virtual BGF cannot reconnect to the gateway controller, it traverses its list of gateway controllers and attempts to connect to one of the gateway controllers. If the virtual BGF finishes traversing its list of gateway controllers, and has not connected to a gateway controller, the virtual BGF waits for a random value between 0 and MWD milliseconds before it begins another attempt to connect to a gateway controller. See section 9.2 of <i>Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005</i> .
<b>Options</b>	<i>milliseconds</i> —Maximum time the virtual BGF waits before contacting a new gateway controller when the connection to the controlling gateway controller is lost. <b>Range:</b> 1 through 36,000 milliseconds <b>Default:</b> 3000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## media

---

<b>Syntax</b>	<pre>media {     rtcp;     rtp; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">monitor</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Enable Real-Time Control Protocol (RTCP) and Real-Time Transport Protocol (RTP) application-level gateways (ALGs) for media flows and monitor packets.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Monitoring RTP and RTCP Traffic in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## mg-maximum-pdu-size

<b>Syntax</b>	mg-maximum-pdu-size { default <i>bytes</i> ; maximum <i>bytes</i> ; minimum <i>bytes</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-properties segmentation</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Set default, maximum, and minimum values for the MG maximum PDU size property of the segmentation package.
<b>Options</b>	<p><b>default <i>bytes</i></b>—Default maximum size of messages that the gateway controller sends to the BGF. <b>Range:</b> 512 through 65,507</p> <p><b>maximum <i>bytes</i></b>—Maximum maximum size of messages that the gateway controller sends to the BGF. <b>Range:</b> 512 through 65,507</p> <p><b>minimum <i>bytes</i></b>—Minimum maximum size of messages that the gateway controller sends to the BGF. <b>Range:</b> 512 through 65,507</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring H.248 Segmentation Properties in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## mg-originated-pending-limit

---

Syntax	<pre>mg-originated-pending-limit {   default <i>number-of-messages</i>;   maximum <i>number-of-messages</i>;   minimum <i>number-of-messages</i>; }</pre>
Hierarchy Level	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">base-root</a> ]
Release Information	Statement introduced in Junos OS Release 8.5. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
Description	Set default, maximum, and minimum values for the MG originated pending limit property of the base root package.
Options	<p><b>default <i>number-of-messages</i></b>—Default number of transaction pending messages that the gateway controller can receive from the virtual BGF. <b>Range:</b> 1 through 512</p> <p><b>maximum <i>number-of-messages</i></b>—Maximum number of transaction pending messages that the gateway controller can receive from the virtual BGF. <b>Range:</b> 1 through 512</p> <p><b>minimum <i>number-of-messages</i></b>—Minimum number of transaction pending messages that the gateway controller can receive from the virtual BGF. <b>Range:</b> 1 through 512</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring H.248 Base Root Properties</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## mg-provisional-response-timer-value

<b>Syntax</b>	mg-provisional-response-timer-value { default <i>milliseconds</i> ; maximum <i>milliseconds</i> ; minimum <i>milliseconds</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">base-root</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Set default, maximum, and minimum values for the MG provisional response timer property of the base root package.
<b>Options</b>	<p><b>default <i>milliseconds</i></b>—Default time within which the gateway controller waits for a pending response from the virtual BGF if a transaction cannot be completed. <b>Range:</b> 500 through 3000</p> <p><b>maximum <i>milliseconds</i></b>—Maximum time within which the gateway controller waits for a pending response from the virtual BGF if a transaction cannot be completed. <b>Range:</b> 500 through 3000</p> <p><b>minimum <i>milliseconds</i></b>—Minimum time within which the gateway controller waits for a pending response from the virtual BGF if a transaction cannot be completed. <b>Range:</b> 500 through 3000</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring H.248 Base Root Properties in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## mg-segmentation-timer

---

<b>Syntax</b>	<pre>mg-segmentation-timer {   default <i>milliseconds</i>;   maximum <i>milliseconds</i>;   minimum <i>milliseconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">segmentation</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Set default, maximum, and minimum values for the MG segmentation timer value property of the segmentation package.
<b>Options</b>	<p><b>default <i>milliseconds</i></b>—Default time within which the gateway controller waits to receive outstanding message segments from the virtual BGF after it receives the SegmentationCompleteToken. <b>Range:</b> 500 through 30000</p> <p><b>maximum <i>milliseconds</i></b>—Maximum time within which the gateway controller waits to receive outstanding message segments from the virtual BGF after it receives the SegmentationCompleteToken. <b>Range:</b> 500 through 30000</p> <p><b>minimum <i>milliseconds</i></b>—Minimum time within which the gateway controller waits to receive outstanding message segments from the virtual BGF after it receives the SegmentationCompleteToken. <b>Range:</b> 500 through 30000</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring H.248 Segmentation Properties in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## mgc-maximum-pdu-size

<b>Syntax</b>	<pre>mgc-maximum-pdu-size {     default <i>bytes</i>;     maximum <i>bytes</i>;     minimum <i>bytes</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-properties segmentation</a> ]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 8.5.</p> <p><b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.</p>
<b>Description</b>	Set default, minimum, and maximum values for the MGC maximum PDU size property of the segmentation package.
<b>Options</b>	<p><b>default <i>bytes</i></b>—Default maximum size of messages that the virtual BGF sends to the gateway controller.</p> <p><b>Range:</b> 512 through 65,507</p> <p><b>maximum <i>bytes</i></b>—Maximum size of messages that the virtual BGF sends to the gateway controller.</p> <p><b>Range:</b> 512 through 65,507</p> <p><b>minimum <i>bytes</i></b>—Minimum maximum size of messages that the virtual BGF sends to the gateway controller.</p> <p><b>Range:</b> 512 through 65,507</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring H.248 Segmentation Properties in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## mgc-originated-pending-limit

---

Syntax	<pre>mgc-originated-pending-limit {   default <i>number-of-messages</i>;   maximum <i>number-of-messages</i>;   minimum <i>number-of-messages</i>; }</pre>
Hierarchy Level	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">base-root</a> ]
Release Information	Statement introduced in Junos OS Release 8.5. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
Description	Set default, maximum, and minimum values for the MGC originated pending limit property of the base root package.
Options	<p><b>default <i>number-of-messages</i></b>—Default number of transaction pending messages that the virtual BGF can receive from the gateway controller. <b>Range:</b> 1 through 512</p> <p><b>maximum <i>number-of-messages</i></b>—Maximum number of transaction pending messages that the virtual BGF can receive from the gateway controller. <b>Range:</b> 1 through 512</p> <p><b>minimum <i>number-of-messages</i></b>—Minimum number of transaction pending messages that the virtual BGF can receive from the gateway controller. <b>Range:</b> 1 through 512</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Configuring H.248 Base Root Properties</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## mgc-provisional-response-timer-value

<b>Syntax</b>	mgc-provisional-response-timer-value { default <i>milliseconds</i> ; maximum <i>milliseconds</i> ; minimum <i>milliseconds</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">services (PGCP)</a> pgcp gateway ( <a href="#">Services PGCP</a> ) <i>gateway-name</i> h248-properties base-root]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Set default, maximum, and minimum values for the MGC provisional response timer value property of the base root package.
<b>Options</b>	<p><b>default <i>milliseconds</i></b>—Default time within which the virtual BGF waits for a pending response from the gateway controller if a transaction cannot be completed. <b>Range:</b> 500 through 3000</p> <p><b>maximum <i>milliseconds</i></b>—Maximum time within which the virtual BGF waits for a pending response from the gateway controller if a transaction cannot be completed. <b>Range:</b> 500 through 3000</p> <p><b>minimum <i>milliseconds</i></b>—Minimum time within which the virtual BGF waits for a pending response from the gateway controller if a transaction cannot be completed. <b>Range:</b> 500 through 3000</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring H.248 Base Root Properties in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## mgc-segmentation-timer

---

<b>Syntax</b>	<pre>mgc-segmentation-timer {   default <i>milliseconds</i>;   maximum <i>milliseconds</i>;   minimum <i>milliseconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">segmentation</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Set default, maximum, and minimum values for the MGC segmentation timer value property of the segmentation package.
<b>Options</b>	<p><b>default <i>milliseconds</i></b>—Default time within which the virtual BGF waits to receive outstanding message segments from the gateway controller after it receives the SegmentationCompleteToken. <b>Range:</b> 500 through 30000</p> <p><b>maximum <i>milliseconds</i></b>—Default time within which the virtual BGF waits to receive outstanding message segments from the gateway controller after it receives the SegmentationCompleteToken. <b>Range:</b> 500 through 30000</p> <p><b>minimum <i>milliseconds</i></b>—Default time within which the virtual BGF waits to receive outstanding message segments from the gateway controller after it receives the SegmentationCompleteToken. <b>Range:</b> 500 through 30000</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring H.248 Segmentation Properties</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## monitor

<b>Syntax</b>	<pre>monitor {   media {     rtcp;     rtp;   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Enable Real-Time Control Protocol (RTCP) and Real-Time Transport Protocol (RTP) application-level gateways (ALGs) for media flows and monitor packets.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Monitoring RTP and RTCP Traffic in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## network-operator-id

<b>Syntax</b>	<code>network-operator-id network-operator-id;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp session-mirroring delivery-function deliver-function-name</a> ], [edit <a href="#">services pgcp gateway (Services PGCP) gateway-name session-mirroring delivery-function deliver-function-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the network operator ID. The BGF includes the network operator ID in the header of mirrored packets that it sends to the delivery function. It is used to identify the operator.
<b>Options</b>	<b>network-operator-id</b> —The network operator ID can be up to five characters.
<b>Required Privilege Level</b>	pgcp-session-mirroring—To view this statement in the configuration. pgcp-session-mirroring-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Session Mirroring in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## no-dscp-bit-mirroring

---

<b>Syntax</b>	no-dscp-bit-mirroring;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">encoding</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Disable mirroring of DSCP bits.
<b>Default</b>	DSCP bits are mirrored by default.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.

## no-rtcp-check

---

<b>Syntax</b>	no-rtcp-check;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">data-inactivity-detection</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Prevent checking for inactivity on RTCP streams.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.

## normal-mg-execution-time

<b>Syntax</b>	<pre>normal-mg-execution-time {     default <i>milliseconds</i>;     maximum <i>milliseconds</i>;     minimum <i>milliseconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> base-root]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Set default, maximum, and minimum values for the normal MG execution time property of the base root package.
<b>Options</b>	<p><b>default <i>milliseconds</i></b>—Default interval within which the gateway controller waits for a response to transactions from the virtual BGF. <b>Range:</b> 500 through 29000</p> <p><b>maximum <i>milliseconds</i></b>—Maximum interval within which the gateway controller waits for a response to transactions from the virtual BGF. <b>Range:</b> 500 through 29000</p> <p><b>minimum <i>milliseconds</i></b>—Minimum interval within which the gateway controller waits for a response to transactions from the virtual BGF. <b>Range:</b> 500 through 29000</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring H.248 Base Root Properties in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## normal-mgc-execution-time

---

<b>Syntax</b>	<pre>normal-mgc-execution-time {     default <i>milliseconds</i>;     maximum <i>milliseconds</i>;     minimum <i>milliseconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> base-root]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Set default, maximum, and minimum values for the normal MGC execution time property of the base root package.
<b>Options</b>	<p><b>default <i>milliseconds</i></b>—Default interval within which the virtual BGF waits for a response to transactions from the gateway controller. <b>Range:</b> 500 through 29000</p> <p><b>maximum <i>milliseconds</i></b>—Maximum interval within which the virtual BGF waits for a response to transactions from the gateway controller. <b>Range:</b> 500 through 29000</p> <p><b>minimum <i>milliseconds</i></b>—Minimum interval within which the virtual BGF waits for a response to transactions from the gateway controller. <b>Range:</b> 500 through 29000</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring H.248 Base Root Properties in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## notification-behavior

---

<b>Syntax</b>	notification-behavior { notification-regulation default (once   0 – 100); }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the default frequency for regulated media inactivity notifications sent by the BGF.
<b>Options</b>	The statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Rate Limiting for the BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## notification-rate-limit

---

<b>Syntax</b>	notification-rate-limit <i>rate</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the maximum notifications sent per second by the PIC or DPC.
<b>Options</b>	<p><b>rate</b>—Maximum number of notifications per second the PIC or DPC sends to a gateway controller.</p> <p><b>Range:</b> 10 through 10,000</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## notification-regulation

---

<b>Syntax</b>	notification-regulation (once   0 – 100);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">notification-behavior</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the default frequency for sending media inactivity notifications for regulated events.
<b>Options</b>	<p><b>once</b>—Send only one media inactivity notification for a regulated event to the gateway controller.</p> <p><b>0 – 100</b>—The percentage of media inactivity notifications for regulated events to send to the gateway controller.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Rate Limiting for the BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## overload-control

---

<b>Syntax</b>	overload-control { <a href="#">queue-limit-percentage</a> <i>percentage</i> ; <a href="#">reject-all-commands-threshold</a> <i>percentage</i> ; <a href="#">reject-new-calls-threshold</a> <i>percentage</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. <b>reject-all-commands-threshold</b> and <b>reject-new-calls-threshold</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Configure the BGF to send overload messages to the gateway controller based on the status of its work queue. The overload messages cause the gateway controller to lower the rate at which it admits packets for processing.
<b>Options</b>	The statement is described separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Overload Control for Voice Calls in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## peak-data-rate

See the following sections:

- [peak-data-rate \(All Streams\)](#) on page 917
- [peak-data-rate \(RTCP\)](#) on page 918

### peak-data-rate (All Streams)

<b>Syntax</b>	<pre>peak-data-rate {   default <i>bytes-per-second</i>;   maximum <i>bytes-per-second</i>;   minimum <i>bytes-per-second</i>; }</pre>
<b>Hierarchy Level</b>	[edit services <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">traffic-management</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Configure the peak data rate for gate streams of any protocol.
<b>Default</b>	<p>The BGF uses the default value of 10,000 bytes per second if the Policy command in H.248 messages is ON and both of the following apply:</p> <ul style="list-style-type: none"> <li>• The peak data rate is not set in the H.248 message.</li> <li>• There is no CLI configuration for peak data rate.</li> </ul>
<b>Options</b>	<p><b>default <i>bytes-per-second</i></b>—Default peak data rate. <b>Range:</b> 125 through 4,294,967,295</p> <p><b>maximum <i>bytes-per-second</i></b>—Maximum peak data rate. <b>Range:</b> 125 through 4,294,967,295</p> <p><b>minimum <i>bytes-per-second</i></b>—Minimum peak data rate. <b>Range:</b> 125 through 4,294,967,295</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Rate Limiting for the BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## peak-data-rate (RTCP)

<b>Syntax</b>	<pre>peak-data-rate {     rtcp (fixed-value <i>bytes</i>   percentage <i>percentage</i>); }</pre>
<b>Hierarchy Level</b>	[edit services <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">traffic-management</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the peak data rate for RTP/RTCP gate streams. You can configure this rate as a fixed value or as a percentage of the RTP gate's rate.
<b>Default</b>	The BGF uses the default value of 5 percent of the RTP gate's rate if the Policy command in H.248 messages in ON and both of the following apply: <ul style="list-style-type: none"><li>• The peak data rate is not set in the H.248 message.</li><li>• There is no CLI configuration for peak data rate.</li></ul>
<b>Options</b>	<p><b>fixed-value</b> —Value entered is a fixed number of bits per second.</p> <p><b><i>bytes-per-second</i></b>—Peak data rate.</p> <p><b>Range:</b> 125 through 4,294,967,295</p> <p><b>percentage</b> —Value entered is a percentage of the RTP gate's rate.</p> <p><b><i>percentage</i></b>—Value entered is a percentage of the RTP's gate rate.</p> <p><b>Range:</b> 0 through 1000</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Rate Limiting for the BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## platform

---

<b>Syntax</b>	platform { device <i>interface-name</i> ; routing-engine; }
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Configure the platform on which the virtual BGF runs. The virtual BGF can run on the Routing Engine or on a Multiservices PIC or MS-DPC. The Multiservices 500 PIC is not supported for virtual BGFs. If you are using high availability, you can configure the virtual BGF to run on a virtual redundant Multiservices PIC (rms) interface
<b>Options</b>	<p><b>device</b>—Causes the virtual BGF to run on a Multiservices PIC, MS-DPC, or an <b>rms</b> interface.</p> <p><b>interface-name</b>—Name of the service interface. If you are using high availability, enter the <b>rms</b> interface number.</p> <p><b>routing-engine</b>—Causes the virtual BGF to run on the Routing Engine. By default, virtual BGFs run on the Routing Engine.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring a Virtual BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## profile-name

---

<b>Syntax</b>	<code>profile-name profile-name;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <a href="#">gateway-name</a> <a href="#">h248-options</a> <a href="#">h248-profile</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Configure the H.248 profile name that the BGF declares in initial registration ServiceChange requests.
<b>Options</b>	<p><b>profile-name</b>—Name of the H.248 profile.</p> <p><b>Syntax:</b> 1-64 bytes in length. The name must start with a letter. Allowed characters are [a-zA-Z0-9_]</p> <p><b>Default:</b> ETSI_BGF, which is the ETSI Ia standard (ETSI ES 283 018 v1.1.4).</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the H.248 Profile in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## profile-version

---

<b>Syntax</b>	<code>profile-version version-number;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <a href="#">gateway-name</a> <a href="#">h248-options</a> <a href="#">h248-profile</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Configure the H.248 profile version that the BGF declares in initial registration ServiceChange requests.
<b>Options</b>	<p><b>version-number</b>—H.248 profile version number.</p> <p><b>Range:</b> 1 through 99</p> <p><b>Default:</b> 1</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the H.248 Profile in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## queue-limit-percentage

---

<b>Syntax</b>	<code>queue-limit-percentage <i>percentage</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">overload-control</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the queue limit percentage (percentage of the maximum work queue size currently in use) that indicates overload. When the gateway controller activates overload control, the BGF generates an overload notification for each transaction on a gate that contains an ADD if the work queue utilization has reach this limit. When 100 percent of the queue is in use, transactions are dropped with error 510 (insufficient resources).
<b>Options</b>	<b><i>percentage</i></b> —Percentage of the overload control work queue in use that triggers creation of an overload notification. <b>Range:</b> 25 through 100 <b>Default:</b> 80
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Overload Control for Voice Calls</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## reconnect

---

<b>Syntax</b>	reconnect (disconnected-900   restart-902);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> <a href="#">control-association-indications</a> <a href="#">disconnect</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Registration Request ServiceChange commands when it attempts to reregister with the gateway controller or register with a new gateway controller after the control association is disconnected.
<b>Default</b>	If you do not specify an option, the virtual BGF includes DC/900 ( <b>disconnected-900</b> ).
<b>Options</b>	<b>disconnected-900</b> —Service restored. The virtual BGF is registering with the last controlling gateway controller following a disconnection of the virtual BGF and gateway controller.  <b>restart-902</b> —Warm boot. The virtual BGF is transitioning to In-Service, and the previously installed state is retained.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## reject-all-commands-threshold

---

<b>Syntax</b>	reject-all-commands-threshold <i>percentage</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> ( <a href="#">PGCP</a> ) pgcp <a href="#">gateway</a> ( <a href="#">Services PGCP</a> ) <i>gateway-name</i> <a href="#">overload-control</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the maximum percentage of the work queue that can be in use before the virtual BGF rejects all non-emergency transactions other than SUBTRACT transactions.
<b>Options</b>	<b><i>percentage</i></b> —Percentage of work queue space used that serves as a threshold for overload control.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Overload Control for Voice Calls in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## reject-new-calls-threshold

---

<b>Syntax</b>	<code>reject-new-calls-threshold <i>percentage</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">overload-control</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the maximum percentage of the work queue that can be in use before the virtual BGF rejects all non-emergency ADD transactions.
<b>Options</b>	<i>percentage</i> —Percentage of work queue space used that serves as a threshold for overload control.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Overload Control for Voice Calls in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## report-service-change

---

<b>Syntax</b>	<code>report-service-change {     service-change-type (forced-906   forced-910); }</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">data-inactivity-detection</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Change the service state of inactive terminations to prevent continued sending of inactivity notifications.
<b>Options</b>	The statement is described separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Latch Deadlock and Media Inactivity Detection in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## request-timestamp

---

<b>Syntax</b>	<code>request-timestamp (requested   suppressed   autonomous);</code>
<b>Hierarchy Level</b>	<code>[edit services pgcp gateway <i>gateway-name</i> h248-properties event-timestamp]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify whether time stamp information is made available to the gateway controller or is suppressed.
<b>Options</b>	<p><b>requested</b>—Enables gateway controller access to time stamp information for notifications.</p> <p><b>suppressed</b>—Disables gateway controller access to time stamp information for notifications.</p> <p><b>autonomous</b>—Equivalent to <b>suppressed</b>.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring H.248 Notification Behavior to Prevent Excessive Media Inactivity Notifications in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## routing-instance

---

<b>Syntax</b>	<pre>routing-instance <i>instance-name</i> {   <b>service-interface</b> <i>interface-name.unit-number</i>; }</pre>
<b>Hierarchy Level</b>	<code>[edit services pgcp <b>virtual-interface</b> <i>interface-name</i>]</code>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 8.4.</p> <p><b>service-interface</b> option introduced in Junos OS Release 9.3.</p>
<b>Description</b>	Map the virtual router interface to a VPN routing and forwarding (VRF) routing instance configured on the router.
<b>Options</b>	<p><b>instance-name</b>—Name of a routing instance that has been configured at the <b>[edit routing-instance]</b> hierarchy level.</p> <p>The remainder of the statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## rtcp

---

<b>Syntax</b>	rtcp;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">monitor</a> <a href="#">media</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Enable Real-Time Control Protocol (RTCP) application-level gateway (ALG) on media flows created when the gateway controller installs media gates on the virtual BGF.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## rtp

---

<b>Syntax</b>	rtp;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">monitor</a> <a href="#">media</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Enable Real-Time Transport Protocol (RTP) application-level gateway (ALG) on media flows created when the gateway controller installs media gates on the virtual BGF.
<b>Required Privilege Level</b>	interface-level—To view this statement in the configuration. interface-level—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## rule

---

<b>Syntax</b>	<pre>rule rule-name {     gateway gateway-name;     nat-pool [ pool-names ]; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp], [edit <a href="#">services</a> service-set service-set-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Specify the rule that the router uses when it applies the NAT pool.
<b>Options</b>	<p><b>rule-name</b>—Identifier for the rule.</p> <p><b>pool-names</b>—Names of one or more NAT pools to be used by the rule.</p> <p><b>Syntax:</b> To specify a list of NAT pools, enclose the NAT pool names in brackets.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## rule-set

---

<b>Syntax</b>	<pre>rule-set rule-set-name {     [rule rule-name] }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp], [edit <a href="#">services</a> service-set service-set-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<p><b>rule-set-name</b>—Identifier for the collection of rules that make up this rule set.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## sbc-utils (Services PGCP)

<b>Syntax</b>	<pre>sbc-utils {   common <i>trace-level</i>;   configuration <i>trace-level</i>;   device-monitor <i>trace-level</i>;   ipc <i>trace-level</i>;   memory-management <i>trace-level</i>;   message <i>trace-level</i>;   minimum <i>trace-level</i>;   user-interface <i>trace-level</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name</a> <a href="#">traceoptions</a> flag]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure trace options for the Signaling Border Controller (SBC) utilities component of the virtual BGF.
<b>Default</b>	<b>warning</b>
<b>Options</b>	<p><b>minimum <i>trace-level</i></b>—Minimum trace level for all <b>sbc-util</b> messages.</p> <p><b>common <i>trace-level</i></b>—Trace level for the common component of SBC utilities.</p> <p><b>configuration <i>trace-level</i></b>—Trace level for the configuration component of SBC utilities.</p> <p><b>device-monitor <i>trace-level</i></b>—Trace level for the device monitor component of SBC utilities.</p> <p><b>ipc <i>trace-level</i></b>—Trace level for the IPC component of SBC utilities.</p> <p><b>memory-management <i>trace-level</i></b>—Trace level for the memory management component of SBC utilities.</p> <p><b>message <i>trace-level</i></b>—Trace level for the message component of SBC utilities.</p> <p><b>user-interface <i>trace-level</i></b>—Trace level for the user interface component of SBC utilities.</p> <p><b><i>trace-level</i></b>—Trace level options are related to the severity of the event being traced. When you choose a trace level, messages at that level and higher levels are captured. Enter one of the following trace levels as the <b><i>trace-level</i></b>:</p> <ul style="list-style-type: none"> <li>• <b>debug</b>—Logging of all code flow of control.</li> <li>• <b>trace</b>—Logging of program trace START and EXIT macros.</li> <li>• <b>info</b>—Summary logs for normal operations, such as the policy decisions made for a call.</li> <li>• <b>warning</b>—Failure recovery or failure of an external entity.</li> <li>• <b>error</b>—Failure with a short-term effect, such as failed processing of a single call.</li> </ul>

**Required Privilege** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.

**Related Documentation** • *Tracing BGF Operations in Session Border Control Solutions Guide Using BGF and IMSG*

---

## segmentation

---

**Syntax**

```
segmentation {  
  mg-segmentation-timer {  
    default milliseconds;  
    maximum milliseconds;  
    minimum milliseconds;  
  }  
  mgc-segmentation-timer {  
    default milliseconds;  
    maximum milliseconds;  
    minimum milliseconds;  
  }  
  mg-maximum-pdu-size {  
    default bytes;  
    maximum bytes;  
    minimum bytes;  
  }  
  mgc-maximum-pdu-size {  
    default bytes;  
    maximum bytes;  
    minimum bytes;  
  }  
}
```

**Hierarchy Level** [edit [services](#) [pgcp](#) [gateway](#) *gateway-name* [h248-properties](#)]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Configure default values for properties in the segmentation package defined in Annex E of *Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005*.

**Options** The statements are explained separately.

**Required Privilege** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.

**Related Documentation** • *Session Border Control Solutions Guide Using BGF and IMSG*

## send-notification-on-delay

---

<b>Syntax</b>	send-notification-on-delay;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">data-inactivity-detection</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Send an inactivity notification immediately when no media packets are detected during a delay period that precedes checking for media inactivity. By default, notifications are sent after both the delay period and an additional period of inactivity have elapsed without any media packets being detected.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">inactivity-delay on page 890</a></li><li>• <a href="#">latch-deadlock-delay on page 894</a></li><li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## service-change

<b>Syntax</b>	<pre> service-change {   control-association-indications {     disconnect {       controller-failure (failover-909   restart-902);       reconnect (disconnected-900   restart-902);     }     down {       administrative (forced-905   forced-908   none);       failure (forced-904   forced-908   none);       graceful (graceful-905   none);     }     up {       cancel-graceful (none   restart-918);       failover-cold (failover-920   restart-901);       failover-warm (failover-919   restart-902);     }   }   virtual-interface-indications {     virtual-interface-down {       administrative (forced-905   forced-906   none);       graceful (graceful-905   none);     }     virtual-interface-up {       cancel-graceful (none   restart-918);       warm (none   restart-900);     }   }   context-indications {     state-loss (forced-910   forced-915   none);   } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of a control association, virtual interface, or context changes.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring the Method and Reason in ServiceChange Commands for Control Associations in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> <li>Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## service-change-type

<b>Syntax</b>	<code>service-change-type (forced-906   forced-910)</code>
<b>Hierarchy Level</b>	[edit <code>services pgcp gateway gateway-name data-inactivity-detection report-service-change</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason used in changing the service state of the termination to active in order to curtail sending of inactivity messages.
<b>Options</b>	<p><b>forced-906</b>—Service is terminated using a forced termination method with reason code 906 (loss of lower layer connectivity).</p> <p><b>forced-910</b>—Service is terminated using a forced termination with reason code 910 (media capability failure).</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Latch Deadlock and Media Inactivity Detection in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## service-interface

<b>Syntax</b>	<code>service-interface interface-name.unit-number;</code>
<b>Hierarchy Level</b>	[edit <code>services pgcp virtual-interface virtual-interface-name routing-instance</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the logical service interface. The NAT routes point to this service interface. This service interface must match the service interface configured in the routing instance.
<b>Options</b>	<b>interface-name.unit-number</b> —Name and logical interface number of the service interface.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the Service Set for Redundant Services PICS in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## service-state

---

See the following sections:

- [service-state \(Virtual BGF\) on page 932](#)
- [service-state \(Virtual Interface\) on page 933](#)

### service-state (Virtual BGF)

<b>Syntax</b>	<code>service-state (in-service   out-of-service-forced   out-of-service-graceful);</code>
<b>Hierarchy Level</b>	[edit <code>services pgcp gateway gateway-name</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Set the service state of the virtual BGF.
<b>Options</b>	<p><b>in-service</b>—The virtual BGF is operational and available for traffic. When the virtual BGF is in service, it attempts to connect to the gateway controller and accepts all PGCP commands from the gateway controller.</p> <p><b>out-of-service-forced</b>—Force the virtual BGF out of service. When the virtual BGF is forced out of service, it immediately removes all gates and disconnects from the gateway controller. The virtual BGF does not attempt to establish a new connection.</p> <p><b>out-of-service-graceful</b>—Cause the virtual BGF to go out of service by entering a draining mode and waiting for all terminations to be subtracted before going out of service. During the draining, the BGF accepts only subtract commands from the gateway controller.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

## service-state (Virtual Interface)

<b>Syntax</b>	<code>service-state (in-service   out-of-service-forced   out-of-service-graceful);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp virtual-interface</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Set the service state of the virtual interface.
<b>Options</b>	<p><b>in-service</b>—Virtual interface is operational and available for traffic. When the virtual interface is in service, it is connected to the physical interface and accepts all Voice calls. This is the default.</p> <p><b>out-of-service-forced</b>—Force the virtual interface out of service. When the virtual interface is forced out of service, it immediately removes all calls and disconnects from the physical interface. The virtual interface does not attempt to establish a new connection.</p> <p><b>out-of-service-graceful</b>—Cause the virtual interface goes out of service by entering a draining mode and waiting for all terminations to be subtracted before going out of service. During the draining, the virtual interface accepts only subtract commands from the gateway controller.</p>
<b>Required Privilege Level</b>	<p>interface-level—To view this statement in the configuration.</p> <p>interface-level—To add this statement to the configuration.</p>

## services (PGCP)

<b>Syntax</b>	<code>services pgcp { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Define service rules to be applied to traffic.
<b>Options</b>	<b>pgcp</b> —Identifier for the PGCP set of rules statements.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>BGF VoIP Solution Overview</i> and <i>IMSG Session Border Control Solution Overview</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## session-mirroring

---

<b>Syntax</b>	<pre>session-mirroring {     <b>delivery-function</b> <i>delivery-function-name</i> {         <b>destination-address</b> <i>destination-address</i>;         <b>destination-port</b> <i>destination-port</i>;         <b>network-operator-id</b> <i>network-operator-id</i>;         <b>source-address</b> <i>source-address</i>;         <b>source-port</b> (<b>Mirrored BGF Packets</b>) <i>source-port</i>;     }     <b>disable-session-mirroring</b>; }</pre>
<b>Hierarchy Level</b>	[edit services pgcp]; [edit services pgcp <b>gateway (Services PGCP)</b> <i>gateway-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the session mirroring feature.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	pgcp-session-mirroring—To view this statement in the configuration. pgcp-session-mirroring-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Session Mirroring Overview and Configuring Session Mirroring in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## source-address

---

<b>Syntax</b>	<pre>source-address <i>source-address</i>;</pre>
<b>Hierarchy Level</b>	[edit services pgcp <b>session-mirroring delivery-function</b> <i>deliver-function-name</i> ], [edit services pgcp <b>gateway (Services PGCP)</b> <i>gateway-name session-mirroring delivery-function</i> <i>deliver-function-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the source address that is applied to mirrored packets.
<b>Options</b>	<b>source-address</b> —Address of the interface on which the BGF sends session-mirroring data to the delivery function.
<b>Required Privilege Level</b>	pgcp-session-mirroring—To view this statement in the configuration. pgcp-session-mirroring-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Session Mirroring Overview and Configuring Session Mirroring in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## source-port (Mirrored BGF Packets)

<b>Syntax</b>	<code>source-port <i>source-port</i>;</code>
<b>Hierarchy Level</b>	[edit services pgcp <a href="#">session-mirroring delivery-function <i>deliver-function-name</i></a> ], [edit services pgcp <a href="#">gateway (Services PGCP) <i>gateway-name</i> session-mirroring delivery-function <i>deliver-function-name</i></a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the source port applied to the mirrored packets.
<b>Options</b>	<b><i>source-port</i></b> —Port on which the BGF sends session-mirroring data to the delivery function. <b>Range:</b> 1 through 65,535
<b>Required Privilege Level</b>	pgcp-session-mirroring—To view this statement in the configuration. pgcp-session-mirroring-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Session Mirroring Overview and Configuring Session Mirroring in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## state-loss

---

<b>Syntax</b>	state-loss (forced-910   forced-915   none);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> <a href="#">context-indications</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Service-Interruption ServiceChange commands that it sends to the gateway controller after a state loss on a specific context.
<b>Default</b>	If you do not specify an option, the virtual BGF includes FO/915 ( <b>forced-915</b> ).
<b>Options</b>	<b>forced-910</b> —State loss because of a media failure. A mismatch between the pgcpd process and the Multiservices PIC or DPC states was detected on one or more of the context's gates.  <b>forced-915</b> —State loss. A mismatch between the pgcpd process and the Multiservices PIC or DPC states was detected on one or more of the context's gates.  <b>none</b> —Virtual BGF does not send a ServiceChange command to the gateway controller.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Session Mirroring Overview in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## stop-detection-on-drop

---

<b>Syntax</b>	stop-detection-on-drop;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">data-inactivity-detection</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the BGF to stop inactivity detection when a gate action is set to drop. When the call is resumed, the BGF starts the delay time and resumes data inactivity detection.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Latch Deadlock and Media Inactivity Detection in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## sustained-data-rate

See the following sections:

- [sustained-data-rate \(All Streams\)](#) on page 937
- [sustained-data-rate \(RTCP Streams\)](#) on page 938

### sustained-data-rate (All Streams)

<b>Syntax</b>	<pre>sustained-data-rate {   default <i>bytes-per-second</i>;   maximum <i>bytes-per-second</i>;   minimum <i>bytes-per-second</i>;   rtcp-include; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">traffic-management</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. <b>maximum</b> and <b>minimum</b> options introduced in Junos OS Release 9.5.
<b>Description</b>	Configure the sustained data rate for streams of any protocol, including RTP.
<b>Default</b>	<p>The BGF uses the default value of 10,000 bytes per second if the Policy command in H.248 messages in ON and both of the following apply:</p> <ul style="list-style-type: none"> <li>• The sustained data rate is not set in the H.248 message.</li> <li>• There is no CLI configuration for sustained data rate.</li> </ul>
<b>Options</b>	<p><b>default <i>bytes-per-second</i></b>—Default value for sustained data rate. <b>Range:</b> 125 through 4,294,967,295</p> <p><b>maximum <i>bytes-per-second</i></b>—Maximum value for sustained data rate. <b>Range:</b> 125 through 4,294,967,295</p> <p><b>minimum <i>bytes-per-second</i></b>—Minimum value for sustained data rate. <b>Range:</b> 125 through 4,294,967,295</p> <p><b>rtcp-include</b>—Include rtcp bandwidth in the sustained data rate.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Rate-Limiting for VoIP Traffic Overview and Configuring Rate Limiting for the BGF</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## sustained-data-rate (RTCP Streams)

<b>Syntax</b>	<pre>sustained-data-rate {     rtcp (fixed-value <i>bytes-per-second</i>   percentage <i>percentage</i>); }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-properties</a> <a href="#">traffic-management</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the sustained data rate for RTP/RTCP gate streams. You can configure this rate as a fixed value or as a percentage of RTP's sustained data rate.
<b>Default</b>	The virtual BGF uses the default value of 5 percent of the RTP gates's rate if the Policy command in H.248 messages in ON and both of the following apply: <ul style="list-style-type: none"><li>• The sustained data rate is not set in the H.248 message.</li><li>• There is no CLI configuration for sustained data rate.</li></ul>
<b>Options</b>	<p><b>fixed-value</b>—Value entered is a fixed number of bits per second.</p> <p><b><i>bytes-per-second</i></b>—Sustained data rate. <b>Range:</b> 125 through 4,294,967,295</p> <p><b><i>percentage bytes-per-second</i></b>—Value entered is a percentage of the RTP's gate rate.</p> <p><b><i>percentage</i></b>—Value entered is a percentage of the RTP's gate rate. <b>Range:</b> 0 through 1000</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Rate-Limiting for VoIP Traffic Overview and Configuring Rate Limiting for the BGF in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## timerx

<b>Syntax</b>	<code>timerx seconds;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-properties hanging-termination-detection</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	<p>Activate and configure hanging termination detection. Setting this timer to a value other than zero (0) activates hanging termination detection. If no messages are exchanged between the BGF and the gateway controller for a termination before this time expires, the BGF sends a notification to the gateway controller. The timer resets when the BGF and the gateway controller exchange a message for the termination. The timer value that you set is the default value, and can be overridden by H.248 messages sent from the gateway controller.</p> <p>Your configuration takes effect on new and modified terminations.</p>
<b>Options</b>	<p><b>seconds</b>—Number of seconds between the last message exchanged for this termination and when the BGF sends a notification to the gateway controller. Setting the timer to zero (0) deactivates hanging termination detection.</p> <p><b>Range:</b> 0 through 2,147,480</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Detecting Hanging Terminations in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## tmax-retransmission-delay

<b>Syntax</b>	<code>tmax-retransmission-delay milliseconds;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-timers</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.4.
<b>Description</b>	Configure the maximum time that a transaction can be kept alive. T-Max is explained in Annex D of <i>Gateway control protocol v3, ITU-T Recommendation H.248.1, September 2005</i> .
<b>Options</b>	<p><b>milliseconds</b>—Duration of the delay before the BGF considers the gateway controller to be down.</p> <p><b>Range:</b> 0 through 65,535</p> <p><b>Default:</b> 25000</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

## traceoptions (Services PGCP)

```
Syntax  traceoptions {
        file <filename filename> <files number> <match regex> <size size> <world-readable |
        no-world-readable>;
        flag {
            bgf-core {
                common trace-level;
                default trace-level;
                firewall trace-level;
                gate-logic trace-level;
                pic-broker trace-level;
                policy trace-level;
                statistics trace-level;
            }
            default trace-level;
            h248-stack {
                control-association trace-level;
                default trace-level;
                messages;
                media-gateway trace-level;
            }
            sbc-utils {
                common trace-level;
                configuration trace-level;
                default trace-level;
                device-monitor trace-level;
                ipc trace-level;
                memory-management trace-level;
                messaging trace-level;
                user-interface trace-level;
            }
        }
    }
```

**Hierarchy Level** [edit [services pgcp](#)]

**Release Information** Statement introduced in Junos OS Release 8.4.  
Statement extensively revised in Junos OS Release 9.5.

**Description** Configure PGCP tracing operations. The messages are output to `/var/log/pgcpd`.

**Options** The statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Tracing BGF Operations in Session Border Control Solutions Guide Using BGF and IMSG*

## traffic-management

```
Syntax traffic-management {
    max-burst-size {
        default bytes-per-second;
        maximum bytes-per-second;
        minimum bytes-per-second;
        rtcp {
            (fixed-value bytes-per-second | percentage percentage);
        }
    }
    peak-data-rate {
        default bytes-per-second;
        maximum bytes-per-second;
        minimum bytes-per-second;
        rtcp {
            (fixed-value bytes-per-second | percentage percentage);
        }
    }
    sustained-data-rate {
        default bytes-per-second;
        maximum bytes-per-second;
        minimum bytes-per-second;
        rtcp {
            (fixed-value bytes-per-second | percentage percentage);
        }
    }
}
```

**Hierarchy Level** [edit services pgcp gateway *gateway-name* h248-properties]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Configure traffic management of the gate stream and the RTCP stream. The parameters for the RTCP stream take effect only when the gate is an RTP/RTCP gate.

**Options** The statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Rate-Limiting for VoIP Traffic Overview and Configuring Rate Limiting for the BGF in Session Border Control Solutions Guide Using BGF and IMSG*

## up

---

<b>Syntax</b>	<pre>up {   cancel-graceful (none   restart-918);   failover-cold (failover-920   restart-901);   failover-warm (failover-919   restart-902); }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> <a href="#">control-association-indications</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Notification Messages or Registration commands in ServiceChange commands when a control association transitions to In-Service.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Control Associations in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## use-lower-case

---

<b>Syntax</b>	<pre>use-lower-case;</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure upper-case encoding for H.248 messages.
<b>Default</b>	By default H.248 messages are encoded in upper case.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

---

## use-wildcard-response

---

<b>Syntax</b>	use-wildcard-response;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Enable the virtual BGF to issue service change commands as wildcard-response commands, which trigger a short response from the gateway controller. If you do not enable the use of wildcard responses for service change commands, the gateway controller will generate an individual response for every termination that matches the service change command.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Enabling Wildcards for ServiceChange Notifications in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## virtual-interface

---

Syntax	<pre>virtual-interface <i>number</i> {   nat-pool [ <i>pool-names</i> ];   routing-instance <i>instance-name</i> {     service-interface <i>interface-name.unit-number</i>;   }   service-state (in-service   out-of-service-forced   out-of-service-graceful); }</pre>
Hierarchy Level	[edit <b>services</b> pgcp]
Release Information	Statement introduced in Junos OS Release 8.4. <b>service-state</b> option introduced in Junos OS Release 9.0. <b>service-interface</b> option introduced in Junos OS Release 9.3.
Description	Configure a virtual interface for the BGF.
Options	<p><b>number</b>—Identifier for the interface. <b>Range:</b> 0 through 1023</p> <p><b>pool-names</b>—Names of one or more NAT pools to be used by the virtual interface. <b>Syntax:</b> To specify a list of NAT pools, enclose the NAT pool names in brackets.</p> <p>The remainder of the statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li><i>Virtual Interfaces with the BGF Overview</i> and <i>Configuring Virtual Interfaces</i> in <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## virtual-interface-down

---

<b>Syntax</b>	virtual-interface-down { administrative (forced-905   forced-906   none); graceful (graceful-905   none); }
<b>Hierarchy Level</b>	[edit <a href="#">services pgcp gateway gateway-name h248-options service-change virtual-interface-indications</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of the virtual interface changes to Out-of-Service.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>

## virtual-interface-indications

---

<b>Syntax</b>	<pre>virtual-interface-indications {   virtual-interface-down {     administrative (forced-905   forced-906   none);     graceful (graceful-905   none);   }   virtual-interface-up {     cancel-graceful (none   restart-918);     warm(none   restart-900);   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in ServiceChange commands that it sends to the gateway controller when the state of the virtual interface changes.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## virtual-interface-up

---

<b>Syntax</b>	<pre>virtual-interface-up {   cancel-graceful (none   restart-918);   warm (none   restart-900); }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> <a href="#">pgcp</a> <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> <a href="#">virtual-interface-indications</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the ServiceChange command that the virtual BGF sends to the gateway controller when the state of the virtual interface changes to In-Service.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces in Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## warm

---

<b>Syntax</b>	warm (none   restart-900);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> pgcp <a href="#">gateway</a> <i>gateway-name</i> <a href="#">h248-options</a> <a href="#">service-change</a> <a href="#">virtual-interface-indications</a> <a href="#">virtual-interface-up</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the method and reason that the virtual BGF includes in Service-Restoration ServiceChange commands that it sends to the gateway controller when a virtual interface transitions to In-Service.
<b>Default</b>	If you do not specify an option, the virtual BGF includes RS/900 ( <b>restart-900</b> ).
<b>Options</b>	<p><b>none</b>—Virtual BGF does not send a ServiceChange command.</p> <p><b>restart-900</b>—Service restored. The virtual interface has become In-Service and is in the Forwarding state.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring the Method and Reason in ServiceChange Commands for Virtual Interfaces in Session Border Control Solutions Guide Using BGF and IMSG</i></li> </ul>



# Service Interface Pools Configuration Guidelines

To configure service interface pools, include the **service-interface-pools** statement at the **[edit services]** hierarchy level:

```
[edit services]
service-interface-pools {
  pool pool-name {
    interface interface-name.unit-number;
  }
}
```

This chapter discusses the following topics that provide information about configuring service interface pools:

- [Configuring Service Interface Pools on page 949](#)

## Configuring Service Interface Pools

---

To configure a service interface pool, include the following statements at the **[edit services service-interface-pools]** hierarchy level:

```
[edit services service-interface-pools]
pool pool-name {
  interface interface-name.unit-number;
}
```



## CHAPTER 36

# Summary of Service Interface Pools Statements

The following sections explain each of the service interface pools statements. The statements are organized alphabetically.

### interface

---

<b>Syntax</b>	<code>interface <i>interface-name.unit-number</i>;</code>
<b>Hierarchy Level</b>	[edit services <a href="#">service-interface-pools</a> <a href="#">pool</a> <i>pool-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Add logical service interfaces to the pool of service interfaces.
<b>Options</b>	<p><i>interface-name.unit-number</i>—Name and logical unit number of the service interface.</p> <ul style="list-style-type: none"><li>• All interfaces in a pool must belong to the same service PIC or DPC.</li><li>• All interfaces assigned to the same service must be in the same pool.</li><li>• Logical interfaces cannot be in more than one pool.</li><li>• All interfaces must have either <b>family inet</b> or <b>family inet6</b> configured.</li><li>• Logical unit 0 cannot be configured in a service interface pool.</li><li>• You can configure up to 1000 logical interfaces in a service interface pool.</li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## pool

---

<b>Syntax</b>	<code>pool pool-name {     interface interface-name.unit-number; }</code>
<b>Hierarchy Level</b>	[edit services <a href="#">service-interface-pools</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure a service interface pool for VPN aggregation for the BGF feature.
<b>Options</b>	<b>pool-name</b> —Name of the service interface pool.  The remaining options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li><i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

## service-interface-pools

---

<b>Syntax</b>	<code>service-interface-pools {     pool pool-name {         interface interface-name.unit-number;     } }</code>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure service interface pools used for VPN aggregation.
<b>Options</b>	The options are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li><i>Session Border Control Solutions Guide Using BGF and IMSG</i></li></ul>

# PTSP Configuration Guidelines

To configure the static policies for the packet-triggered subscribers and policy control (PTSP) feature, include the **ptsp** statement at the **[edit services]** hierarchy level:

```
[edit services]
ptsp {
  rule rule-name {
    count-type (application | rule);
    demux (destination-address | source-address);
    forward-rule forward-rule-name;
    match-direction (input | input-output | output);
    term precedence {
      from {
        application-group-any;
        application-groups [ application-group-name ];
        applications [ application-name ];
        local-port-range low low-value high high-value;
        local-ports [ value-list ];
        protocol protocol-number;
        remote-address address <except>;
        remote-address-range low low-value high high-value <except>;
        remote-port-range low low-value high high-value;
        remote-ports [ value-list ];
        remote-prefix-list prefix-list-name <except>;
      }
      then {
        (accept | discard);
        count (application | application-group | application-group-any | rule | none);
        forwarding-class forwarding-class;
        police policer-name;
      }
    }
  }
}
rule-set rule-set-name {
  rule rule-name;
}
forward-rule rule-name {
  term precedence {
    from {
      application-groups [ application-group-name ];
      applications [ application-name ];
      local-address address <except>;
      local-address-range low low-value high high-value <except>;
```

```
local-prefix-list prefix-list-name <except >;  
}  
then {  
  forwarding-instance forwarding-instance unit-number unit-number;  
}  
}  
}
```



**NOTE:** Starting with Junos OS Release 12.1, offloading is supported by the packet-triggered subscribers and policy control (PTSP) plug-in. Offloading is accomplished using the Juniper Forwarding Mechanism (JFM) on all MX Series routers with Modular Port Concentrators (MPCs). The `show services subscriber flows client-id client-id` command displays the offload status. For more information about offloading, see [“Local Policy Decision Function Configuration Guidelines” on page 1079](#)

---

For information about using the PTSP statements to configure the PTSP feature, see the *Junos OS Subscriber Management and Services Library*.

## CHAPTER 38

# Summary of PTSP Configuration Statements

- [application-group-any](#) on page 956
- [application-groups](#) on page 956
- [applications \(Services PTSP\)](#) on page 957
- [count-type](#) on page 957
- [demux](#) on page 958
- [forward-rule \(Configuring\)](#) on page 959
- [forward-rule \(Including in Rule\)](#) on page 960
- [from \(Forward Rule\)](#) on page 960
- [from \(Rule\)](#) on page 961
- [local-address](#) on page 962
- [local-address-range](#) on page 963
- [local-port-range](#) on page 963
- [local-ports](#) on page 964
- [local-prefix-list](#) on page 964
- [match-direction \(Services PTSP\)](#) on page 965
- [protocol](#) on page 965
- [remote-address](#) on page 966
- [remote-address-range](#) on page 967
- [remote-port-range](#) on page 967
- [remote-ports](#) on page 968
- [remote-prefix-list](#) on page 968
- [rule \(Configuring\)](#) on page 969
- [rule \(Including in Rule Set\)](#) on page 970
- [rule-set \(Services PTSP\)](#) on page 970
- [services \(PTSP\)](#) on page 971
- [term \(Forward Rule\)](#) on page 972

- [term \(Rule\) on page 973](#)
- [then \(Forward Rule\) on page 974](#)
- [then \(Rule\) on page 975](#)

---

## application-group-any

---

<b>Syntax</b>	application-group-any;
<b>Hierarchy Level</b>	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify that any application group defined in the database is considered a match.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

---

## application-groups

---

<b>Syntax</b>	application-group [ <i>application-group-name</i> ];
<b>Hierarchy Level</b>	[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> <a href="#">from</a> ] [edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Identify one or more application groups defined in the application identification configuration for inclusion as a match condition.
<b>Options</b>	<i>application-group-name</i> —Identifier of the application group.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## applications (Services PTSP)

<b>Syntax</b>	<code>applications [ <i>application-name</i> ];</code>
<b>Hierarchy Level</b>	<code>[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> <b>from</b>]</code> <code>[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <b>from</b>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Identify one or more applications defined in the application identification configuration for inclusion as a match condition.
<b>Options</b>	<b><i>application-name</i></b> —Identifier of the application.
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> </ul>

## count-type

<b>Syntax</b>	<code>count-type (application   rule);</code>
<b>Hierarchy Level</b>	<code>[edit services ptsp <b>rule</b> <i>rule-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the statistics aggregation, collection, and reporting style for this rule. Terms and rules cannot mix and match different styles. All service rules attached to a given service set must have the same style.
<b>Options</b>	<p><b><i>application</i></b>—Report statistics in a flat file and aggregate them by application for one of the following:</p> <ul style="list-style-type: none"> <li>An application, where the count action <b><i>application</i></b> is specified in the term.</li> <li>An application group, where the count action <b><i>application-group</i></b> is specified in the term.</li> <li>All application groups, where the count action <b><i>application-group-any</i></b> is specified in the term.</li> </ul> <p><b><i>rule</i></b>—Aggregate statistics for the service rule. The statistics are reported by Diameter. All count actions in all terms for the rule must specify <b><i>rule</i></b>.</p>
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> </ul>

## demux

---

<b>Syntax</b>	demux (destination-address   source-address);
<b>Hierarchy Level</b>	[edit services ptsp <b>rule</b> rule-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the IP address used to establish the subscriber context. Subscriber instantiation is always triggered for ingress packets, so this value indicates which IP address in the ingress packets for the flow is used. If the IP address does not correspond to a known subscriber, then a new subscriber context is created. All service rules attached to a given service set must have the same setting.
<b>Options</b>	<b>destination-address</b> —Use the destination IP address field of the ingress packet header for the flow.  <b>source-address</b> —Use the source IP address field of the ingress packet header for the flow.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## forward-rule (Configuring)

<b>Syntax</b>	<pre> forward-rule <i>forward-rule-name</i> {   term <i>precedence</i> {     from {       application-groups [ <i>application-group-name</i> ];       applications [ <i>application-name</i> ];       local-address <i>address</i> &lt;except&gt;;       local-address-range low <i>low-value</i> high <i>high-value</i> &lt;except &gt;;       local-prefix-list <i>prefix-list-name</i> &lt;except &gt;;     }     then {       forwarding-instance <i>forwarding-instance</i>;       unit-number <i>unit-number</i>;     }   } } </pre>
<b>Hierarchy Level</b>	[edit services ptsp]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the forwarding instance for a specific subscriber or set of subscribers based on the IP address, network, or prefix list. The rule match is applied on the input side.
<b>Options</b>	<p><b><i>forward-rule-name</i></b>—Identifier for the collection of terms that constitute this rule.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> </ul>

## forward-rule (Including in Rule)

---

<b>Syntax</b>	<code>forward-rule <i>forward-rule-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services ptsp <b>rule</b> <i>rule-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Identify the forwarding instance for inclusion in a rule.
<b>Options</b>	<b><i>forward-rule-name</i></b> —Identifier for the forward rule that specifies the forwarding instance.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## from (Forward Rule)

---

<b>Syntax</b>	<pre>from {   <b>application-groups</b> [ <i>application-group-name</i> ];   <b>applications</b> [ <i>application-name</i> ];   <b>local-address</b> <i>address</i> &lt;except &gt;;   <b>local-address-range</b> low <i>low-value</i> high <i>high-value</i> &lt;except &gt;;   <b>local-prefix-list</b> <i>prefix-list-name</i> &lt;except &gt;; }</pre>
<b>Hierarchy Level</b>	<code>[edit services ptsp forward-rule <i>forward-rule-name</i> <b>term</b> <i>precedence</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify match conditions for the PTSP term.
<b>Options</b>	For information on match conditions, see the description of firewall filter match conditions in the <i>Routing Policy Feature Guide for Routing Devices</i> .  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## from (Rule)

<b>Syntax</b>	<pre> from {   application-group-any;   application-groups [ application-group-name ];   applications [ application-name ];   local-port-range low low-value high high-value;   local-ports [ value-list ];   protocol protocol-number;   remote-address address &lt;except &gt;;   remote-address-range low low-value high high-value &lt;except &gt;;   remote-port-range low low-value high high-value;   remote-ports [ value-list ];   remote-prefix-list prefix-list-name &lt;except &gt;; } </pre>
<b>Hierarchy Level</b>	[edit services ptsp rule <i>rule-name</i> <b>term</b> <i>precedence</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify match conditions for the PTSP term.
<b>Options</b>	<p>For information on match conditions, see the description of firewall filter match conditions in the <i>Routing Policy Feature Guide for Routing Devices</i>.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> </ul>

## local-address

---

<b>Syntax</b>	<code>local-address (address   any-unicast) &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the address for rule matching. Local address values are matched against a source or destination IP address for the flow depending on the configured value for the <b>demux</b> statement. If you do not specify an address, then any local address matches this term. If you do not specify a prefix value, then a host mask is the default.
<b>Options</b>	<b>address</b> —IPv4 or IPv6 address or prefix value.  <b>any-unicast</b> —Match all unicast addresses.  <b>except</b> —(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li><li>• <a href="#">demux on page 958</a></li></ul>

## local-address-range

<b>Syntax</b>	<code>local-address-range low <i>low-value</i> high <i>high-value</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	<code>[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> <a href="#">from</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the address range for rule matching. Local address values are matched against a source or destination IP address for the flow depending on the configured value for the <b>demux</b> statement. If you do not specify an address, then any local address matches this term.
<b>Options</b>	<p><b><i>low-value</i></b>—Lower boundary for the IPv4 or IPv6 address range.</p> <p><b><i>high-value</i></b>—Upper boundary for the IPv4 or IPv6 address range.</p> <p><b><i>except</i></b>—(Optional) Exclude the specified address range from rule matching.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> <li>• <a href="#">demux on page 958</a></li> </ul>

## local-port-range

<b>Syntax</b>	<code>local-port-range low <i>low-value</i> high <i>high-value</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <a href="#">from</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the port range for rule matching.
<b>Options</b>	<p><b><i>low-value</i></b>—Lower boundary for the port range.</p> <p><b><i>high-value</i></b>—Upper boundary for the port range.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> </ul>

## local-ports

---

<b>Syntax</b>	<code>local-ports [ <i>port-numbers</i> ];</code>
<b>Hierarchy Level</b>	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <b>from</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Identify one or more ports for inclusion as a match condition.
<b>Options</b>	<i>port-numbers</i> —Port number.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## local-prefix-list

---

<b>Syntax</b>	<code>local-prefix-list <i>prefix-list-name</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> <b>from</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the [edit policy-options] hierarchy level.
<b>Options</b>	<i>prefix-list-name</i> —Prefix list.  <b>except</b> —(Optional) Exclude the specified prefix list from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## match-direction (Services PTSP)

---

<b>Syntax</b>	<code>match-direction (input   input-output   output);</code>
<b>Hierarchy Level</b>	[edit services ptsp <b>rule</b> <i>rule-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the direction in which the rule match is applied.
<b>Options</b>	<p><b>input</b>—Apply the rule match on the input side of the interface.</p> <p><b>input-output</b>—Apply the rule match bidirectionally.</p> <p><b>output</b>—Apply the rule match on the output side of the interface.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> </ul>

## protocol

---

<b>Syntax</b>	<code>protocol <i>protocol-number</i>;</code>
<b>Hierarchy Level</b>	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <b>from</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Identify the protocol for inclusion as a match condition.
<b>Options</b>	<b><i>protocol-number</i></b> —Protocol number.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> </ul>

## remote-address

---

<b>Syntax</b>	<code>remote-address (<i>address</i>   any-unicast) &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the address for rule matching. Remote address values are matched against a destination or source IP address for the flow depending on the configured value for the <b>demux</b> statement. If you do not specify an address, then any remote address matches this term. If you do not specify a prefix value, then a host mask is the default.
<b>Options</b>	<b>address</b> —IPv4 or IPv6 address or prefix value.  <b>any-unicast</b> —Match all unicast addresses.  <b>except</b> —(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules</i> in <i>Junos OS Subscriber Management and Services Library</i></li><li>• <a href="#">demux on page 958</a></li></ul>

## remote-address-range

<b>Syntax</b>	<code>remote-address-range low <i>low-value</i> high <i>high-value</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	<code>[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <a href="#">from</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the address range for rule matching. Remote address values are matched against a destination or source IP address for the flow depending on the configured value for the <b>demux</b> statement. If you do not specify an address, then any remote address matches this term.
<b>Options</b>	<p><b><i>low-value</i></b>—Lower boundary for the IPv4 or IPv6 address range.</p> <p><b><i>high-value</i></b>—Upper boundary for the IPv4 or IPv6 address range.</p> <p><b><i>except</i></b>—(Optional) Exclude the specified address range from rule matching.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> <li>• <a href="#">demux on page 958</a></li> </ul>

## remote-port-range

<b>Syntax</b>	<code>remote-port-range low <i>low-value</i> high <i>high-value</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <a href="#">from</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the port range for rule matching.
<b>Options</b>	<p><b><i>low-value</i></b>—Lower boundary for the port range.</p> <p><b><i>high-value</i></b>—Upper boundary for the port range.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li> </ul>

## remote-ports

---

<b>Syntax</b>	<code>remote-ports [ <i>port-numbers</i> ];</code>
<b>Hierarchy Level</b>	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <b>from</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Identify one or more ports for inclusion as a match condition.
<b>Options</b>	<i>port-numbers</i> —Port number.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## remote-prefix-list

---

<b>Syntax</b>	<code>remote-prefix-list <i>prefix-list-name</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> <b>from</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the [edit policy-options] hierarchy level.
<b>Options</b>	<i>prefix-list-name</i> —Prefix list.  <b>except</b> —(Optional) Exclude the specified prefix list from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## rule (Configuring)

**Syntax**

```
rule rule-name {
  count-type (application | rule);
  demux (destination-address | source-address);
  forward-rule forward-rule-name;
  match-direction (input | input-output | output);
  term precedence {
    from {
      application-group-any;
      application-groups [ application-group-name ];
      applications [ application-name ];
      local-port-range low low-value high high-value;
      local-ports [ value-list ];
      protocol protocol-number;
      remote-address address <except>;
      remote-address-range low low-value high high-value <except>;
      remote-ports [ value-list ];
      remote-port-range low low-value high high-value;
      remote-prefix-list prefix-list-name <except>;
    }
    then {
      (accept | discard);
      count (application | application-group | application-group-any | rule | none);
      forwarding-class forwarding-class;
      police policer-name;
    }
  }
}
```

**Hierarchy Level** [edit services ptsp]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Specify the rule the router uses when applying this service.

**Options** *rule-name*—Identifier for the collection of terms that constitute this rule.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library*

## rule (Including in Rule Set)

---

<b>Syntax</b>	<code>rule rule-name;</code>
<b>Hierarchy Level</b>	<code>[edit services ptsp rule-set rule-set-name]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the rule the router uses when applying this service.
<b>Options</b>	<b>rule-name</b> —Identifier for the collection of terms that constitute this rule.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## rule-set (Services PTSP)

---

<b>Syntax</b>	<code>rule-set rule-set-name {     [rule rule-names ]; }</code>
<b>Hierarchy Level</b>	<code>[edit services ptsp]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<b>rule-set-name</b> —Identifier for the collection of rules that constitute this rule set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## services (PTSP)

---

<b>Syntax</b>	<code>services ptsp { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Define the services to be applied to traffic.
<b>Options</b>	<b>ptsp</b> —Identify the values configured for PTSP matching rules.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## term (Forward Rule)

---

**Syntax**    `term precedence {  
              from {  
                  application-groups [ application-group-name ];  
                  applications [ application-name ];  
                  local-address address <except>;  
                  local-address-range low low-value high high-value <except>;  
                  local-prefix-list prefix-list-name <except>;  
              }  
              then {  
                  forwarding-instance forwarding-instance;  
                  unit-number unit-number;  
              }  
          }`

**Hierarchy Level**    [edit services ptsp **forward-rule** forward-rule-name]

**Release Information**    Statement introduced in Junos OS Release 10.2.

**Description**    Define the term properties for the forward rule.

**Options**    *precedence*—Precedence value for this term in relation to other terms. Term with lowest precedence is evaluated first.

The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • *Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library*

## term (Rule)

```
Syntax  term precedence {
        from {
            application-group-any;
            application-groups [ application-group-name ];
            applications [ application-name ];
            local-port-range low low-value high high-value;
            local-ports [ value-list ];
            protocol protocol-number;
            remote-address address <except>;
            remote-address-range low low-value high high-value <except>;
            remote-port-range low low-value high high-value;
            remote-ports [ value-list ];
            remote-prefix-list prefix-list-name <except>;
        }
        then {
            (accept | discard);
            count (application | application-group | application-group-any | rule);
            forwarding-class forwarding-class;
            police policer-name;
        }
    }
```

**Hierarchy Level** [edit services ptsp **rule** *rule-name*]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Define the term properties for the PTSP rule.

**Options** **precedence**—Precedence value for this term in relation to other terms. Term with lowest precedence is evaluated first.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library*

## then (Forward Rule)

---

<b>Syntax</b>	<pre>then {     forwarding-instance <i>forwarding-instance</i>;     unit-number <i>unit-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit services ptsp forward-rule <i>forward-rule-name</i> <b>term</b> <i>precedence</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Define the term actions for the forward rule.
<b>Options</b>	<p><b><i>forwarding-instance</i></b>—Identifier for the forwarding instance for packet flows accepted under this policy.</p> <p><b><i>unit-number</i></b>—Unit number associated with the forwarding instance.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library</i></li></ul>

## then (Rule)

<b>Syntax</b>	<pre> then {   (accept   discard);   count (application   application-group   application-group-any   rule);   forwarding-class <i>forwarding-class</i>;   police <i>policer-name</i>; } </pre>
<b>Hierarchy Level</b>	[edit services ptsp rule <i>rule-name</i> <b>term</b> <i>precedence</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Define the term actions. You can configure the router to accept or discard the targeted traffic. The action modifiers (count and forwarding-class) are optional.
<b>Options</b>	<p>You can configure one of the following actions:</p> <ul style="list-style-type: none"> <li>• <b>accept</b>—Accept the packets and all subsequent packets in flows that match the rules.</li> <li>• <b>discard</b>—Discard the packet and all subsequent packets in flows that match the rules.</li> </ul> <p>When you select <b>accept</b> as the action, you can optionally configure one or both of the following action modifiers. No action modifiers are allowed with the <b>discard</b> action.</p> <ul style="list-style-type: none"> <li>• <b>count (application   application-group   application-group-any   rule   none)</b>—For all accepted packets that match the rules, record a packet count using PTSP statistics practices. You can specify one of the following options; there is no default setting: <ul style="list-style-type: none"> <li>• <b>application</b>—Count the application that matched in the <b>from</b> clause.</li> <li>• <b>application-group</b>—Count the application group that matched in the <b>from</b> clause.</li> <li>• <b>application-group-any</b>—Count all application groups that match <b>from</b> <b>application-group-any</b> under the <b>any</b> group name.</li> <li>• <b>rule</b>—Count the rule that matched in the <b>from</b> clause.</li> <li>• <b>none</b>—Same as not specifying <b>count</b> as an action.</li> </ul> </li> <li>• <b>forwarding-class <i>forwarding-class</i></b>—Specify the forwarding class name for outgoing packets.</li> </ul> <p>When you include a policer, the only allowed action is <b>discard</b>. For more information on policers, see the <i>Routing Policy Feature Guide for Routing Devices</i>.</p> <ul style="list-style-type: none"> <li>• <b>police <i>policer-name</i></b>—Apply rate-limiting properties to the traffic as configured at the [edit firewall policer <i>policer-name</i>] hierarchy level. This configuration allows bit-rate and burst-size attributes to be applied to the traffic that are not supported by PTSP rules.</li> </ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

- Related Documentation**
- *Configuring Static PTSP Rules in Junos OS Subscriber Management and Services Library*

## PART 3

# Junos Application Aware

- [Junos Application Aware Overview on page 979](#)
- [Application Identification Configuration Guidelines on page 993](#)
- [Summary of Application Identification Configuration Statements on page 1013](#)
- [Application-Aware Access List Configuration Guidelines on page 1057](#)
- [Summary of AACL Configuration Statements on page 1067](#)
- [Local Policy Decision Function Configuration Guidelines on page 1079](#)
- [Summary of L-PDF Configuration Statements on page 1087](#)



# Junos Application Aware Overview

This chapter describes several related features that support application-level filtering and per-subscriber, per-application group bandwidth control as an extension of Intrusion Detection and Prevention (IDP). In addition to IDP, the main components are application identification (APPID), application-aware access list (AACL) services, and local policy decision functionality for application-related services (L-PDF).



**NOTE:** Starting with Junos OS Release 12.1, all interface-style services are supported for dynamic Point-to-Point Protocol over Ethernet (PPPoE) subscribers on all MX Series routers with modular Modular Port Concentrators (MPCs).



**NOTE:** Because the Junos OS extension-provider package framework lacks aggressive constraint checks, you should not set the `policy-db-size` statement at the `[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]` hierarchy level to a high value. For Junos Application Aware (previously known as Dynamic Application Awareness) configurations, the recommended values for the extension-provider package options at this hierarchy level are as follows:

- `control-cores = 1`
- `data-cores = 7`
- `object-cache-size = 1280` (for Multiservices 400 PIC and Multiservices DPC)
- `policy-db-size = 200`
- Include these package values: `jservices-idp`, `jservices-appid`, `jservices-llpdf`, `jservices-aacl`

For more information about this configuration, see the following topics in the *SDK Applications Configuration Guide and Command Reference*:

- *Configuring Control and Data Cores*
- *Configuring Memory Settings*
- *Configuring Packages on the PIC*



**NOTE:** In the export version of JUNOS, signature download is not expected to work for AppID and IDP features in the Junos Application Aware (previously known as Dynamic Application Awareness) suite. In order to make it work, you must additionally install the Crypto Software Suite.

This chapter includes the following:

- [IDP Overview on page 980](#)
- [APPID Overview on page 982](#)
- [AACL Overview on page 984](#)
- [L-PDF Overview on page 986](#)
- [Configuring Multiple IDP Detectors on page 988](#)
- [Best-Effort Application Identification of DPI-Serviced Flows on page 988](#)

---

## IDP Overview



**NOTE:** Starting with Junos OS Release 12.1, all interface-style services are supported for dynamic Point-to-Point Protocol over Ethernet (PPPoE) subscribers on all MX Series routers with modular Modular Port Concentrators (MPCs).

The Junos Application Aware (previously known as Dynamic Application Awareness for the Junos OS) set of services adds support for the intrusion detection and prevention (IDP) functionality using Deep Packet Inspection (DPI) technology to Juniper Networks MX Series 3D Universal Edge Routers equipped with Multiservices Dense Port Concentrators (MS-DPCs) and M120 or M320 Multiservices Edge Routers equipped with Multiservices 400 PICs.

The IDP functionality is already supported on Juniper Networks J Series Services Routers and SRX Series Services Gateways running the Junos OS and is described in the *Junos OS Security Configuration Guide*. Starting with Junos OS Release 11.3, support for the IDP functionality is extended to T320, T640, and T1600 routers. In addition, multiple IDP detectors are now supported on the M120, M320, and MX Series routers with Enhanced III Flexible PIC Concentrators (FPCs).



**NOTE:** In the export version of JUNOS, signature download is not expected to work for AppID and IDP features in Junos Application Aware. In order to make it work, you must additionally install the Crypto Software Suite.

The same CLI statements and commands are used on all platforms with the following caveats:

- **Service sets**—IDP is incorporated as a component of service sets only on the specified Juniper Networks T Series, M Series and MX Series routers. IDP depends on application

identification services (APPID) for definition and detection of some Layer 7 applications. Before configuring an IDP policy, you must download the APPID application package. Only one service set can be applied to a single interface when the APPID functionality is used.

- **Multiple IDP detectors**—Except for the maximum number of decoder binary instances (4) that are loaded into the process space, multiple IDP detectors on the M120, M320, and MX Series routers function in a similar way to the existing IDP detector support on J Series and SRX Series devices. To view the current policy and the corresponding detector version, use the **show security idp status detail** command.

To configure IDP properties, include statements at the **[edit security idp]** hierarchy level. In general, you configure IDP processes by including the **idp-policy** statement at the **[edit system processes]** hierarchy level. For use in T Series, M Series and MX Series applications, you then reference this configuration by including the **idp-profile** statement at the **[edit services service-set]** hierarchy level. To configure SNMP IDP objects, include the **idp** statement at the **[edit snmp health-monitor]** hierarchy level. The operational commands for monitoring and regulating IDP activity are the **clear security idp**, **request security idp**, and **show security idp** commands.

To configure the source IP address for downloading security packages, use the command **set security idp security-package source-address ip-address** because it is not possible to download security packages if the router uses private addressing on its outgoing interface. The source address should be a valid IP address on the node.



**NOTE:** On T Series, M Series and MX Series routers, the IDP **ip-action** statement is supported on TCP, UDP, and ICMP flows. When the **ip-action target** is **service**, the **ip-action** flow is applied if the traffic matches the values specified for the source port, destination port, source address, and destination address. However, for ICMP flows, the destination port is 0, so that any ICMP flow matching the source port, source address, and destination address would be blocked. For more information about the **ip-action** statement, see the *Junos OS CLI Reference*.

When the Multiservices PIC configured for a service set is either administratively taken offline or undergoes a failure, all the traffic entering the configured interface with an IDP service set would be dropped without notification. To avoid this traffic loss, include the **bypass-traffic-on-pic-failure** statement at the **[edit services service-set service-set-name service-set-options]** hierarchy level. When this statement is configured, the affected packets are forwarded in the event of a Multiservices PIC failure or offlining, as though interface-style services were not configured.



**NOTE:** Data channel applications for protocols such as FTP, TFTP, RTSP, and SIP are not in the same application group as their control channel applications. For example, control channel application **junos:ftp** is in the group **junos:file-server** but the corresponding data application **junos:system:ftp-data** is not in any group.



**NOTE:** Because the extension-provider package framework lacks aggressive constraint checks, you should not set the `policy-db-size` statement at the `[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]` hierarchy level to a high value. For Junos Application Aware configurations, the recommended values for the extension-provider package options at this hierarchy level are as follows:

- `control-cores = 1`
- `data-cores = 7`
- `object-cache-size = 1280` (for Multiservices 400 PIC and Multiservices DPC)
- `policy-db-size = 200`
- Include these package values: `jservices-idp`, `jservices-appid`, `jservices-llpdf`, `jservices-aacl`

For more information about this configuration, see the following topics in the *SDK Applications Configuration Guide and Command Reference*:

- *Configuring Control and Data Cores*
- *Configuring Memory Settings*
- *Configuring Packages on the PIC*

---

**Related Documentation**

- [Configuring Multiple IDP Detectors on page 988](#)

---

## APPID Overview



**NOTE:** Starting with Junos OS Release 12.1, all interface-style services are supported for dynamic Point-to-Point Protocol over Ethernet (PPPoE) subscribers on all MX Series routers with modular Modular Port Concentrators (MPCs).

The APPID feature identifies applications as constituents of application groups in TCP/UDP/ICMP traffic. It is supported on MX Series routers equipped with Multiservices DPCs and on M120 or M320 routers equipped with Multiservices 400 PICs and Aggregated Multiservices (AMS) PICs. Aggregated Multiservices PICs (`ams-` interfaces) enable multiple `ms-` interfaces to be grouped together in a single bundle and cause the traffic destined for this AMS group to be distributed over the member services PICs of the group. Junos OS Trio chipsets enable the calculation of a symmetric hash for the forward and reverse flows, and support a microcode map in the forwarding plane. This capability enables load-balancing of traffic across various services PICs in an AMS group. Starting with Junos OS Release 12.1, `ams-` interfaces enable an N:1 redundancy mechanism to cluster together N number of `ms-` interfaces in an AMS group that supports load sharing.



**NOTE:** For ams- interfaces and rms- interfaces, the statistics data in the bulk statistics file is collected using the reports received from the MS PICs. For the ams- interfaces, the retrieval and storage of statistics is not possible because of multiple PICs containing statistics data for the same subscriber. For interfaces in an AMS group, statistics data from different MS PICs in the AMS group are collected and aggregated on the Routing Engine where a timer control is activated and the data is saved in the bulkstats file based on this timer. This method of collection causes the statistics data in the bulkstats file to be displayed with a small delay period.

To configure APPID, include statements at the **[edit services application-identification]** hierarchy level to specify parameter values for defining applications, enable or disable application rules, and gather the applications and rules into groups.

The following are related operational commands:

- **show/clear application-identification application-system-cache**
- **show/clear application-identification counters**

For more information on the CLI configuration, see the *Application Identification*. For more information on the operational commands, see the [CLI Explorer](#).



**NOTE:** Because the extension-provider package framework lacks aggressive constraint checks, you should not set the **policy-db-size** statement at the **[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]** hierarchy level to a high value. For Junos Application Aware (previously known as Dynamic Application Awareness) configurations, the recommended values for the extension-provider package options at this hierarchy level are as follows:

- **control-cores = 1**
- **data-cores = 7**
- **object-cache-size = 1280** (for Multiservices 400 PIC and Multiservices DPC)
- **policy-db-size = 200**
- Include these package values: **jservices-idp**, **jservices-appid**, **jservices-llpdf**, **jservices-aacl**

For more information about this configuration, see the following topics in the *SDK Applications Configuration Guide and Command Reference*:

- *Configuring Control and Data Cores*
- *Configuring Memory Settings*
- *Configuring Packages on the PIC*



**NOTE:** In the export version of JUNOS, signature download is not expected to work for AppID and IDP features in Junos Application Aware. In order to make it work, you must additionally install the Crypto Software Suite.

#### Related Documentation

- [Defining an Application Identification on page 995](#)
- [Configuring APPID Rules on page 997](#)
- [Application Identification for Nested Applications on page 1002](#)
- [Configuring Global APPID Properties on page 1004](#)
- [Examples: Configuring Application Identification Properties on page 1010](#)
- [\[edit services application-identification\] Hierarchy Level](#)

---

## AACL Overview



**NOTE:** Starting with Junos OS Release 12.1, all interface-style services are supported for dynamic Point-to-Point Protocol over Ethernet (PPPoE) subscribers on all MX Series routers with modular Modular Port Concentrators (MPCs).

The application-aware access list (AACL) service adds support for a new service that uses application names and groups as matching criteria for filtering traffic. AACL is a stateless, rules-based service that must be combined with application identification to enable policies to be applied to flows based on application and application group membership in addition to traditional packet matching rules. It is supported on MX Series routers equipped with Multiservices DPCs and on M120 or M320 routers equipped with Multiservices 400 PICs. Starting with Junos OS Release 11.3, AACL is supported on T320, T640, and T1600 routers also.

AACL is configured in a similar way to other rules-based services such as Network Address Translation (NAT), class of service (CoS), and stateful firewall. To configure AACL, include rule specifications for match criteria and actions at the **[edit services aacl]** hierarchy level. You can chain AACL rules along with other service rules by including them in a service-set definition at the **[edit services service-set]** hierarchy level, as previously documented.

There is one pair of related operational commands, **show/clear application-aware-access-list statistics**.

For more information on the CLI configuration, see the *Application-Aware Access List*. For more information on the operational command, see the [CLI Explorer](#).



**NOTE:** Because the Junos OS extension-provider package framework lacks aggressive constraint checks, you should not set the `policy-db-size` statement at the `[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]` hierarchy level to a high value. For Junos Application Aware (previously known as dynamic application awareness) configurations, the recommended values for the extension-provider options at this hierarchy level are as follows:

- `control-cores = 1`
- `data-cores = 7`
- `object-cache-size = 1280` (for Multiservices 400 PIC and Multiservices DPC)
- `policy-db-size = 200`
- Include these package values: `jservices-idp`, `jservices-appid`, `jservices-llpdf`, `jservices-aacl`

For more information about this configuration, see the following topics in the *SDK Applications Configuration Guide and Command Reference*:

- *Configuring Control and Data Cores*
- *Configuring Memory Settings*
- *Configuring Packages on the PIC*

#### Related Documentation

- [Configuring AAACL Rules on page 1058](#)
- [Configuring AAACL Rule Sets on page 1062](#)
- [Configuring Logging of AAACL Flows on page 1063](#)
- [Example: Configuring AAACL Rules on page 1064](#)

## L-PDF Overview

---



**NOTE:** Starting with Junos OS Release 12.1, all interface-style services are supported for dynamic Point-to-Point Protocol over Ethernet (PPPoE) subscribers on all MX Series routers with modular Modular Port Concentrators (MPCs).

Starting with Junos OS Release 12.1, the local policy decision function (L-PDF) plug-in can offload flows to the Packet Forwarding Engine. Offloading is supported only on MX Series routers with Modular Port Concentrators (MPCs) and accomplished using the Juniper Forwarding Mechanism (JFM). JFM allows services flows to be offloaded to the Packet Forwarding Engine. However, 5-tuple flows cannot be offloaded. Apart from the local L-PDF plug-in, offloading is supported on the packet-triggered subscribers and policy control (PTSP) plug-in. The `show services application-aware-access-list flows subscriber subscriber-name` command displays offload status.

Local policy decision functionality for application-related services adds support for a new process that regulates collection of statistics related to applications and application groups and tracking of information about dynamic subscribers and static interfaces. This functionality is collectively named the local policy decision function (L-PDF). L-PDF is supported on:

- MX Series routers equipped with Multiservices DPCs.
- M120 or M320 routers equipped with Multiservices 400 PICs.
- Aggregated Multiservices (AMS) PICs.

Multiple `ms-` interfaces can be bundled together in an AMS PIC interface, which causes the traffic destined for this AMS group to be distributed over the member services PICs of the group. Junos OS Trio chipsets enable the calculation of a symmetric hash for the forward and reverse flows, and support a microcode map in the forwarding plane. This capability enables load-balancing of traffic across various services PICs in an AMS group. Starting with Junos OS Release 12.1, `ams-` interfaces enable an N:1 redundancy mechanism to cluster together N number of **`ms-` interfaces** in an AMS group that supports load sharing.

Starting with Junos OS Release 11.3, local L-PDF that resides on the services PIC is supported on T320, T640, and T1600 routers. The application identification (APPID) service defines the applications and how they are grouped. The application-aware access list (AACL) service defines the applications and application groups for which statistics are collected for a specific user or interface. The L-PDF configuration defines the way in which the statistics are output.

To configure properties for statistics output, include the **`policy-decision-statistics-profile`** statement at the **`[edit accounting-options]`** hierarchy level. A new **`traceoptions`** configuration is available at the **`[edit system services local-policy-decision-function]`** hierarchy level. To configure a dynamic profile to attach a specified service set to an interface, include the **`service`** statement at the **`[edit dynamic-profiles profile-name]`**

`interfaces interface-name unit logical-unit-number family inet`] hierarchy level. To attach a service set to a static interface, include the `service-set service-set-name` statement at the `[edit interfaces interface-name unit logical-unit-number family inet service (input | output)]` hierarchy level. For more information on service sets, see *Service Set Properties*.

The following related operational commands are supported:

- `show services local-policy-decision-function flows`
- `show/clear services local-policy-decision-function statistics`
- `show/clear services application-aware-access-list statistics`

For more information on the CLI configuration, see the *Local Policy Decision Function*. For more information on the operational commands, see the [CLI Explorer](#).



**NOTE:** Because the Junos OS extension-provider package (variously known as JSF, MP-SDK, and eJunos in releases earlier than 12.3) lacks aggressive constraint checks, you should not set the `policy-db-size` statement at the `[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]` hierarchy level to a high value. For Junos Application Aware (previously known as Dynamic Application Awareness) configurations, the recommended values for the extension-provider package options at this hierarchy level are as follows:

- `control-cores = 1`
- `data-cores = 7`
- `object-cache-size = 1280` (for Multiservices 400 PIC and Multiservices DPC)
- `policy-db-size = 200`
- Include these package values: `jservices-idp`, `jservices-appid`, `jservices-llpdf`, `jservices-aacl`
- *Configuring Control and Data Cores*
- *Configuring Memory Settings*
- *Configuring Packages on the PIC*

For more information about this configuration, see the following topics in the *SDK Applications Configuration Guide and Command Reference*:

#### Related Documentation

- [Best-Effort Application Identification of DPI-Serviced Flows on page 988](#)
- [Configuring Statistics Profiles on page 1079](#)
- [Applying L-PDF Profiles to Service Sets on page 1083](#)
- [Tracing L-PDF Operations on page 1084](#)

## Configuring Multiple IDP Detectors

---

To configure multiple IDP detectors:

1. In configuration mode, go to the **[edit security]** hierarchy level:

```
user@host# edit security
```

2. Go to the **[edit security idp sensor-configuration flow]** hierarchy level:

```
[edit security]
user@host# edit idp sensor-configuration flow
```

3. Configure the **no-reset-on-policy** statement:

```
[edit security idp sensor-configuration flow]
user@host# set no-reset-on-policy
```

4. Verify the configuration:

```
[edit security]
user@host# show security
idp {
    sensor-configuration {
        flow {
            no-reset-on-policy;
        }
    }
}
```

**Related Documentation**

- [IDP Overview on page 980](#)

## Best-Effort Application Identification of DPI-Serviced Flows

---

This topic describes the following information:

- [Features that Support Application-Level Filtering on page 988](#)
- [Best-Effort Application Determination on page 989](#)
- [APPID, AACL, and L-PDF Processing in Preconvergence Scenarios on page 989](#)

### Features that Support Application-Level Filtering

On MX Series routers equipped with Multiservices DPCs and M120 or M320 routers equipped with Multiservices 400 PICs, Intrusion Detection and Prevention (IDP) is accomplished by Deep Packet Inspection (DPI) of TCP, UDP, and ICMP flows. The application identification (APPID) feature defines applications as members of application groups in TCP/UDP/ICMP traffic. IDP depends on APPID for identification and detection of some Layer 7 applications.

The application-aware access list (AACL) service uses application names and groups as matching criteria for filtering traffic. The service defines the applications and application groups for which statistics are collected for a specific user or interface.

The local policy decision function (L-PDF) enables you to configure properties for statistics output. L-PDF supports a process that regulates collection of statistics related to applications and application groups and tracking of information about dynamic subscribers and static interfaces.

## Best-Effort Application Determination

Typically, APPID conclusively determines the Layer 7 application associated with a given DPI-serviced flow. In these cases, the application identification is final. Occasionally, APPID is only able to make an initial, inconclusive determination of the Layer 7 application associated with a given flow. This is referred to as a "best-effort" application identification. In such cases, the APPID process continues processing packets on that flow and might subsequently make a conclusive determination of the application associated with that flow. In some cases of best-effort application identification, the flow ends before a final application determination can be made.

## APPID, AACL, and L-PDF Processing in Preconvergence Scenarios

The following sections describe APPID, AACL, and L-PDF processing in various stages of application identification for a DPI-serviced flow of TCP/UDP/ICMP traffic.

- [Prior to a Final or Best-Effort Application Identification on page 989](#)
- [Upon Best-Effort Application Identification on page 989](#)
- [While Application Identification Is on a Best-Effort Basis on page 990](#)
- [If a Flow Ends Before an Application Identification Is Made on page 990](#)
- [If a Flow Ends While Application Identification on a Best-Effort Basis on page 990](#)

### Prior to a Final or Best-Effort Application Identification

During the time that APPID has not yet made either a final or best-effort determination of the application associated with a given flow, the flow does not contribute to any per-subscriber or per-application statistics collection.

The output of the following operational mode commands includes flows for which APPID has not yet made either a final or best-effort determination of the associated application:

- **show services local-policy-decision-function flows** (interface *interface-name* | subscriber *subscriber-name*)
- **show services application-aware-access-list flows** (interface *interface-name* | subscriber *subscriber-name*)

In the command output, the **Action** field displays "accept" and the **Application** or **Application group** field displays "unknown" for a flow for which APPID has not yet made either a final or best-effort determination of the associated application.

### Upon Best-Effort Application Identification

When a best-effort application determination is made, AACL does not apply any AACL term actions configured for that flow. There are a number of reasons for this, one being that the action itself (such as "discard") could make a final application determination impossible. Instead, AACL or L-PDF tracks the flow and accepts all packets for that flow

until a final determination is made, at which time the normal ACL or L-PDFL actions are fully applied to the flow.

#### While Application Identification Is on a Best-Effort Basis

During the time that APPID identification of the application associated with a given flow is on a best-effort basis, the flow does not contribute to any per-subscriber or per-application statistics collection.

The output of the following operational mode commands includes flows for which APPID has only made a best-effort determination of the associated application:

- **show services local-policy-decision-function flows** (interface *interface-name* | subscriber *subscriber-name*)
- **show services application-aware-access-list flows** (interface *interface-name* | subscriber *subscriber-name*)

In the command output, the **Action** field displays "accept" and the **Application** or **Application group** field displays "unknown" for a flow for which APPID has only made a best-effort determination of the associated application.

#### If a Flow Ends Before an Application Identification Is Made

If a flow ends before APPID has made either a final or a best-effort application identification, ACL or L-PDF uses the "unknown" application ID as a final determination and performs any necessary collection, aggregation, and reporting of statistics based on that Layer 7 application. In particular, if the **count** ACL term action is configured for the "application-group-any" application, then the statistics for that flow will be collected and aggregated against the count bucket type, and reported as such.

#### If a Flow Ends While Application Identification on a Best-Effort Basis

If a flow ends while the application identification is on a best-effort basis, ACL or L-PDF uses that best-effort determination as a final determination. ACL or L-PDF performs any necessary collection, aggregation, and reporting of statistics based on that Layer 7 application. In particular, if the **count** ACL term action is configured for that Layer 7 application, then the statistics for the flow will be collected and aggregated against the ACL or L-PDF statistics. However, in the case of nested applications, ACL and L-PDF will not consider the best-effort determination as final and the nested application will be reported as an unknown application.

#### **Related Documentation**

- [Configuring ACL Rules on page 1058](#)
- [Configuring Statistics Profiles on page 1079](#)
- [aacl-fields on page 1088](#)
- [aacl-statistics-profile on page 1089](#)
- [rule on page 1072](#)
- [services on page 1073](#)
- [term on page 1076](#)

- [then on page 1077](#)



# Application Identification Configuration Guidelines

To configure application identification services (APPID), include the **application-identification** statement at the **[edit services]** hierarchy level:

```
[edit services]
application-identification {
  application application-name {
    disable;
    idle-timeout seconds;
    index number;
    session-timeout seconds;
    type type;
    type-of-service service-type;
    port-mapping {
      port-range {
        tcp (port | range);
        udp (port | range);
      }
      disable;
    }
  }
}
application-group group-name {
  application-groups {
    name [application-group-name];
  }
  applications {
    name [application-name];
  }
  index number;
  disable;
}
application-system-cache-timeout seconds;
enable-heuristics
max-checked-bytes bytes;
min-checked-bytes bytes;
nested-application
nested-application-settings
no-application-identification;
no-application-system-cache;
no-clear-application-system-cache;
```

```

no-protocol-method;
no-signature-based;
profile profile-name {
  [ rule-set rule-set-name ];
}
rule rule-name {
  disable;
  address address-name {
    destination {
      ip address</prefix-length>;
      port-range {
        tcp [ ports-and-port-ranges ];
        udp [ ports-and-port-ranges ];
      }
    }
    source {
      ip address</prefix-length>;
      port-range {
        tcp [ ports-and-port-ranges ];
        udp [ ports-and-port-ranges ];
      }
    }
    order number;
  }
  application application-name;
}
rule-set rule-set-name {
  rule application-rule-name;
}
signature-method-all-ports
traceoptions {
  file filename <files number> <match regex> <size size> <world-readable |
    no-world-readable>;
  flag flag;
  no-remote-trace;
}
}

[edit services]
hcm {
  url-rule url-rule-name {
    term term-num {
      from {
        url-list url-list-name ;
        url url_identifier {
          host hostname ;
          request-url page-name ;
        }
      }
      then {
        discard;
        accept;
        count;
        log-request;
      }
    }
  }
}

```

```

    }
    url-rule-set url-rule-set-name {
        url-rule rule1;
        url-rule rule2;
    }
}

```

This chapter contains the following sections:

- [Defining an Application Identification on page 995](#)
- [Configuring APPID Rules on page 997](#)
- [Using Stateful Firewall Rules to Identify Data Sessions on page 999](#)
- [Configuring Application Profiles on page 1001](#)
- [Configuring Application Groups on page 1001](#)
- [Application Identification for Nested Applications on page 1002](#)
- [Disabling Application Identification for Nested Applications on page 1004](#)
- [Configuring Global APPID Properties on page 1004](#)
- [Configuring Automatic Download of Application Package Updates on page 1005](#)
- [Configuring APPID Support for Heuristics on page 1006](#)
- [Configuring APPID Support for Unidirectional Traffic on page 1007](#)
- [Tracing APPID Operations on page 1008](#)
- [Examples: Configuring Application Identification Properties on page 1010](#)

## Defining an Application Identification

To configure a specific IP address or port-based application identification, include the **application *application-name*** statement at the **[edit services application-identification]** hierarchy level:

```

application application-name {
    disable;
    idle-timeout seconds;
    index number;
    session-timeout seconds;
    type type;
    type-of-service service-type;
    port-mapping {
        port-range {
            tcp [ ports-and-port-ranges ];
            udp [ ports-and-port-ranges ];
        }
        disable;
    }
}

```

You can include the following general properties in the configuration:

- **application**—Application name, a required statement; maximum 31 characters. Predefined applications have the prefix **junos-** to avoid conflict with user-defined ones.
- **idle-timeout**—Amount of time that a session remains idle before it is deleted.
- **index**—Application index number in the range from 1 through 65,534, with integers 1 through 1024 reserved for predefined applications.
- **session-timeout**—Lifetime of a session.
- **type**—Well known applications, such as HTTP or FTP.
- **type-of-service**—Type of service, defined by service objective. There is no default value; options are **maximize-reliability**, **maximize-throughput**, **minimize-delay**, and **minimize-monetary-cost**.
- **disable**—Disable this application definition in the APPID service.



**NOTE:** You can also specify session and idle timeout values globally for a Multiservices interface by including the following statements at the **[edit interfaces *interface-name* services-options]** hierarchy level:

- **inactivity-non-tcp-timeout**—Inactivity timeout period for non-TCP established sessions.
- **inactivity-tcp-timeout**—Inactivity timeout period for TCP established sessions.
- **session-timeout**—Lifetime of a session.
- **disable-global-timeout-override**—Disallow overriding a global inactivity or session timeout.

You can include the following port-mapping properties at the **[edit services application-identification port-mapping]** hierarchy level:

- **port-range**—TCP or UDP port number or numeric range, entered as **[*minimum-value* – *maximum-value*]**. For port-mapping configurations, this entry is required if the parent node exists.
- **disable**—Disable port-mapping properties for this application.



**NOTE:** For applications with signatures for both client-to-server and server-to-client directions, the APPID for Junos Application Aware (previously known as Dynamic Application Awareness) must accept the data packets in both directions on the same session to complete the identification process.

For a configuration example, see [“Examples: Configuring Application Identification Properties” on page 1010](#).

- Related Documentation**
- [APPID Overview on page 982](#)
  - [Configuring APPID Rules on page 997](#)
  - [Using Stateful Firewall Rules to Identify Data Sessions on page 999](#)
  - [Configuring Application Profiles on page 1001](#)
  - [Configuring Application Groups on page 1001](#)
  - [Tracing APPID Operations on page 1008](#)
  - [\[edit services application-identification\] Hierarchy Level](#)

## Configuring APPID Rules

This configuration specifies the properties for identifying an application for which a source or destination IP address and port is used for a known application, without the requirement of an application signature. For example, the Session Initiation Protocol (SIP) server initiates a session from its identified port, 5060. You can therefore specify the SIP server IP address and port 5060 in the port mapping configuration for the SIP application. The advantage of using this method is to provide efficiency and accuracy of application identification for your network.

To configure application rule properties, include the **rule** statement at the **[edit services application-identification]** hierarchy level:

```
rule rule-name {
  address address-name {
    destination {
      ip address</prefix-length>;
      port-range {
        tcp [ ports-and-port-ranges ];
        udp [ ports-and-port-ranges ];
      }
    }
    source {
      ip address</prefix-length>;
      port-range {
        tcp [ ports-and-port-ranges ];
        udp [ ports-and-port-ranges ];
      }
    }
    order number;
  }
  application application-name;
  disable;
}
```

You can include the following application rule properties:

- **address**—Address properties for APPID rule processing. This statement is mandatory; you must specify either destination or source properties.
- **destination**—Destination address and port information. The **ip** statement defines the IP address and netmask (IPv4 only), and the **port-range** statement defines the TCP or UDP port number or numeric range, entered as *[minimum-value – maximum-value]*.
- **source**—Source address and port information. The **ip** statement defines the IP address and netmask (IPv4 only), and the **port-range** statement defines the TCP or UDP port number or numeric range, entered as *[minimum-value – maximum-value]*.
- **order**—Application matching priority. For address configurations, the order number resolves the conflict when multiple address entries are matched for a specific session; the lower the number, the higher the priority. This statement is mandatory and must contain a unique value.
- **application**—Name of the application to be included in the rule.
- **disable**—Disable processing for this application rule.

The **rule-set** statement defines a collection of APPID rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the **rule-set** statement at the **[edit services application-identification]** hierarchy level with a **rule** statement for each rule:

```
rule-set rule-set-name {  
    rule application-rule-name;  
}
```

**Related  
Documentation**

- [APPID Overview on page 982](#)
- [Defining an Application Identification on page 995](#)
- [Using Stateful Firewall Rules to Identify Data Sessions on page 999](#)
- [Configuring Application Profiles on page 1001](#)
- [Configuring Application Groups on page 1001](#)
- [Examples: Configuring Application Identification Properties on page 1010](#)

## Using Stateful Firewall Rules to Identify Data Sessions

The APPID configuration properties enable the Junos OS to detect applications based on signatures, ports, and addresses. For signature-based detection, most of the protocol control sessions are identified, but data sessions are not identified. For example, APPID identifies FTP connections to port 21 (FTP control sessions); however, FTP can open child/data sessions to transfer files and data. These sessions are not identified by signature-based APPID because they do not have well-defined signatures.

Application-level gateways (ALGs) configured using stateful firewall rules can assist APPID in identifying these data sessions. These sessions include file and video transfers that are heavy consumers of bandwidth, so a mechanism for policing and classifying this traffic effectively is a useful tool. In addition to FTP, this mechanism applies to TFTP and RTSP traffic.

To incorporate the stateful firewall rules into Junos Application Aware (previously known as Dynamic Application Awareness for Junos OS) sessions, include the following configurations:

1. Include the stateful firewall package at the **[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]** hierarchy level:  

```
package jservices-sfw;
```
2. Define two stateful firewall rules as shown in the following example, one to identify the appropriate ALGs for FTP, TFTP, or RTSP traffic and the other to allow all traffic:



**NOTE:** Session Initiation Protocol (SIP) is already covered by APPID and the SIP ALG is not supported by stateful firewall, hence a SIP configuration is not needed.

```
[edit services]
stateful-firewall {
  rule rule1 {
    match-direction input-output;
    term term1 {
      from {
        applications [ junos-ftp junos-tftp junos-rtsp ];
      }
      then {
        accept;
      }
    }
  }
  rule rule2 {
    match-direction input-output;
    term term1 {
      then {
        accept;
      }
    }
  }
}
```

```

    }
    rule-set rs1 {
        rule rule1;
        rule rule2;
    }
}

```



**NOTE:** The existing AACL and L-PDF operational mode commands should report the new applications when they are identified.

3. Attach the stateful firewall rule set to a service set, as shown in the following example:

```

service-set test-chaining {
    application-identification-profile add-based;
    stateful-firewall-rule-sets rs1;
    idp-profile idp1;
    aacl-rules rule1;
    interface-service {
        service-interface ms-2/0/0.0;
    }
}

```

4. Include *no-drop* settings for stateful firewall and TCP, as needed.

Stateful firewall processing drops packets in a number of scenarios:

- TCP sessions do not start with a SYN flag. (This prevents sessions from resuming; otherwise, when the PIC starts for the first time, all existing TCP sessions in flight will be dropped).
- If the TCP tracker detects SYN but no SYN/ACK or only an ACK, then the ACK is dropped. There are a number of similar checks to verify the TCP connection, window checks, and so forth.
- TCP checks for stateful firewall are aggressive when ALGs are run. It is not possible to ignore TCP errors when an ALG is run on a session.
- If an ALG detects malformed packets (for example, if the FTP PORT command is not RFC-compliant), it drops packets. If an ALG is not able to allocate resources, it drops packets.

You can include the settings shown in the following example to assist in controlling these packet drops:

```

[edit interfaces]
ms-1/2/0 {
    services-options {
        ignore-errors {
            tcp;
            alg;
        }
    }
}

```

The **tcp** statement mediates the first two issues listed, with reference to TCP SYN detection. The **alg** statement handles the fourth issue. ALGs require strict TCP processing, which cannot be relaxed.

- Related Documentation**
- [APPID Overview on page 982](#)
  - [Defining an Application Identification on page 995](#)
  - [Application Identification for Nested Applications on page 1002](#)
  - [Configuring Global APPID Properties on page 1004](#)
  - [Tracing APPID Operations on page 1008](#)

---

## Configuring Application Profiles

You can define an application profile for use in a service set. The profile consists of one or more rule sets, but only one profile can be included per service set.

To specify the application profile constituents, include the **profile** statement at the **[edit services application-identification]** hierarchy level:

```
profile profile-name {  
  [ rule-set rule-set-name ];  
}
```

You assign a profile name and include one or more predefined rule sets. For more information on rule sets, see “[Configuring APPID Rules](#)” on page 997. You can then include the profile in a service-set definition:

```
[edit services]  
service-set service-set-name {  
  profile profile-name;  
}
```

The definitions specific to Junos Application Aware (previously known as Dynamic Application Awareness) include the APPID and IDP profiles and the AACL rule set. For more information on service sets, see *Service Set Properties*.

- Related Documentation**
- [APPID Overview on page 982](#)
  - [Defining an Application Identification on page 995](#)
  - [Configuring Application Groups on page 1001](#)
  - [Configuring Global APPID Properties on page 1004](#)

---

## Configuring Application Groups

You can define an application group to process a number of applications or subgroups at the same time. To configure application group properties, include the **application-group** statement at the **[edit services application-identification]** hierarchy level:

```
application-group group-name {
```

```
application-groups {  
    application-group-name;  
}  
applications {  
    application-name;  
}  
index number;  
disable;  
}
```

You can include the following application group properties:

- **applications**—List of applications to include in this application group. The **name** statement is mandatory and must include at least one entry.
- **application-groups**—List of application groups to include in a larger application group. The **name** statement is mandatory and must include at least one entry.
- **index**—Application group index number in the range from 1 through 65,534. This mandatory value must be unique.
- **disable**—Disable processing for this application group.

**Related  
Documentation**

- [Defining an Application Identification on page 995](#)
- [Configuring APPID Rules on page 997](#)
- [Configuring Application Profiles on page 1001](#)
- [Configuring Global APPID Properties on page 1004](#)
- [Examples: Configuring Application Identification Properties on page 1010](#)

---

## Application Identification for Nested Applications

The application identification feature is used by intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports. *Nested applications* are protocols running over the parent application. For example, both Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications. To do this, the application layer is split into two layers: Layer 7 applications and Layer 7 protocols.

The predefined application signatures included with Junos OS have been created to detect the Layer 7 nested applications. Predefined application signatures can be used in attack objects.

To configure nested application properties, include the **nested-application** statement at the **[edit services application-identification]** hierarchy level:

```
nested-application name {  
    index number;  
    protocol protocol;  
    signature name {  
        chain-order;  
        maximum-transactions number;  
    }  
}
```

```

    member name {
        context (http-header-content-type | http-header-host | http-url-parsed |
            http-url-parsed-param-parsed);
        direction (any | client-to-server | server-to-client);
        pattern dfa-pattern;
    }
    order number;
}
type type;
}

```

You can include the following application rule properties:

- **chain-order**—Signatures can contain multiple members. If the chain order feature is on, those members are read in order. The default for this option is no chain order. If a signature contains only one member, this option is ignored.
- **context**—Define a service specific context. The options are **http-header-content-type**, **http-header-host**, **http-url-parsed**, **http-url-parsed-param-parsed**. This statement is mandatory.
- **direction**—The connection direction of the packets to apply pattern matching. The options are **client-to-server**, **server-to-client**, or **any**. This statement is mandatory.
- **index**—A number that is a one-to-one mapping to the application name that is used to ensure that each signature definition is unique. The index range for predefined applications is 1 through 32767. The index range for custom applications and custom nested applications is 32768 through 65534.
- **maximum transactions**—The maximum number of transactions that should occur before a match is made. This statement is mandatory.
- **member**—Define a member name for a custom nested application signature definition. Custom definitions can contain multiple members that define attributes for an application.
- **order**—Define application matching priority. For address configurations, the order number resolves the conflict when multiple address entries are matched for a specific session. The lower number has higher priority. This statement is mandatory.
- **pattern**—Define an attack pattern to be detected. This statement is mandatory.
- **protocol**—The protocol that will be monitored to identify nested applications. The value **http** is supported. This statement is mandatory.
- **signature**—Name of the custom nested application signature definition. Must be a unique name with a maximum length of 32 characters. This statement is mandatory.
- **type**—Well-known application name for this application definition, such as Facebook or Kazza. This application name must be unique with a maximum length of 32 characters. This statement is mandatory.

#### Related Documentation

- [APPID Overview on page 982](#)
- [Defining an Application Identification on page 995](#)
- [Disabling Application Identification for Nested Applications on page 1004](#)

- [Configuring Global APPID Properties on page 1004](#)
- [Tracing APPID Operations on page 1008](#)

## Disabling Application Identification for Nested Applications

---

Sometimes there is a need to identify multiple different applications running on the same Layer 7 protocols. For example, both Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications. To do this, the application layer is split into two layers: Layer 7 applications and Layer 7 protocols. Application identification for nested applications is turned on by default. You can manually turn it off by using the CLI.

To disable nested application identification:

- Set the **no-nested-application** statement.

```
[edit services application-identification nested-application-settings]  
user@host# no-nested-application
```

To verify the configuration, issue the **show services application-identification nested-application-settings** command.

To reenable nested application identification:

- Delete the **no-nested-application** statement.

```
[edit services application-identification nested-application-settings]  
user@host# delete services application-identification nested-application-settings  
no-nested-application
```

If you are finished configuring the device, commit the configuration.

### Related Documentation

- [APPID Overview on page 982](#)
- [Application Identification for Nested Applications on page 1002](#)

## Configuring Global APPID Properties

---

You can define additional properties that apply on a global basis to APPID processing and are not part of a specific application, group, rule, or profile definition. To configure these global APPID properties, include the following statements at the **[edit services application-identification]** hierarchy level:

```
application-identification {  
  application-system-cache-timeout seconds;  
  max-checked-bytes bytes;  
  min-checked-bytes bytes;  
  nested-application name  
  nested-application-settings  
  no-application-identification  
  no-application-system-cache;
```

```

no-clear-application-system-cache;
no-protocol-method;
no-signature-based;
signature-method-all-ports;
}

```

The global application properties have the following effect:

- **application-system-cache-timeout**—Lifetime for system cache entries, in seconds.
- **max-checked-bytes**—The maximum number of bytes to be inspected in APPID processing, in the range from 0 through 100,000 bytes.
- **min-checked-bytes**—The minimum number of bytes to be inspected in APPID processing, in the range from 0 through 2000 bytes.
- **nested-application**—Configure a custom nested application definition for the desired application name that will be used by the system to identify the nested application as it passes through the device. For more information see [nested-application](#).
- **nested-application-settings**—Configure nested application options for application identification services. For more information see [nested-application-settings](#).
- **no-application-identification**—Disable all application identification methods.
- **no-application-system-cache**—Disable storing application identification results in the application system cache.
- **no-clear-application-system-cache**—Disable clearing the application system cache.
- **no-protocol-method**—Disable the protocol-based application identification method, which is enabled by default.
- **no-signature-based**—Disable the signature-based application identification method.
- **signature-method-all-ports**—Run signature matching on all traffic.

#### Related Documentation

- [APPID Overview on page 982](#)
- [Defining an Application Identification on page 995](#)
- [Application Identification for Nested Applications on page 1002](#)
- [Disabling Application Identification for Nested Applications on page 1004](#)
- [Tracing APPID Operations on page 1008](#)
- [Examples: Configuring Application Identification Properties on page 1010](#)

## Configuring Automatic Download of Application Package Updates

You can set up automatic downloading of application package updates. To configure downloads, include the **download** statement at the **[edit services application-identification]** hierarchy level:

```

download {
  automatic {
    interval hour;
  }
}

```

```
    start-time time;  
  }  
  url url;  
}
```

You can include the following download statements:

- **download**—Define download properties.
- **automatic**—Set **start-time** value and **interval** in hours for automatic downloads. The default **start-time** is **0:00** and the range is from 0:00 through 24:00. The default **interval** is **24** and the range is from 1 through 168.
- **url**—Specify the download URL.

**Related  
Documentation**

- [APPID Overview on page 982](#)
- [Defining an Application Identification on page 995](#)
- [Examples: Configuring Application Identification Properties on page 1010](#)

---

## Configuring APPID Support for Heuristics

---

Heuristics methodology provides a mechanism for identifying encrypted data packets in point-to-point applications. These packets are not normally detected by the existing application signatures.

To enable APPID to employ heuristics in traffic identification:

1. Include the **enable-heuristics** statement:

```
[edit services application-identification]  
user@host# enable-heuristics
```

The **show services application-identification counter** operational command includes additional output fields that report the number of encrypted sessions.



**NOTE:** When you enable heuristics, performance and scaling values might be negatively affected. This mechanism assists the APPID module in identifying encrypted traffic, but only if the identifications are supported by the current signature package.

---

**Related  
Documentation**

- [APPID Overview on page 982](#)
- [Defining an Application Identification on page 995](#)
- [Application Identification for Nested Applications on page 1002](#)
- [Configuring Global APPID Properties on page 1004](#)
- [Configuring APPID Support for Unidirectional Traffic on page 1007](#)
- [Examples: Configuring Application Identification Properties on page 1010](#)

## Configuring APPID Support for Unidirectional Traffic

With asymmetrical routing, a networking device sees only one side of the network sessions, either from client to server or from server to client. Additional functionality is required to support application identification with unidirectional traffic. This addition enables a session for a specified service set to support an asymmetrical routing environment, and allows complete application matches using existing application signatures for traffic in the client-to-server direction only.

To enable APPID to support application matching on unidirectional traffic:

1. Include the **support-uni-directional-traffic** statement:

```
[edit services service-set service-set-name service-set-options]
user@host# support-uni-directional-traffic
```

This enables the session belonging to the specified service set to support the asymmetrical routing environment. The APPID module then reports complete matches for the unidirectional traffic.

2. Include the **enable-asymmetric-traffic-processing** statement:

```
[edit services service-set service-set-name service-set-options]
user@host# enable-asymmetric-traffic-processing
```

This enables the framework and plug-in to handle unidirectional traffic at a service-set level.

When you enable these settings, APPID treats unidirectional TCP traffic like a UDP connection. UDP traffic itself does not receive any special treatment because the service PIC cannot determine whether UDP traffic is unidirectional or bidirectional. The settings do not affect processing of sessions created with bidirectional traffic.

If the traffic includes both unidirectional and bidirectional sessions, the APPID module uses heuristics to decide whether to change the reporting logic.



**NOTE:** This feature does not change the processing for any services except APPID. However, other services, including stateful firewall, AACL, and IDP, can process unidirectional traffic in a limited manner.

### Related Documentation

- [APPID Overview on page 982](#)
- [Defining an Application Identification on page 995](#)
- [Application Identification for Nested Applications on page 1002](#)
- [Configuring Global APPID Properties on page 1004](#)
- [Configuring APPID Support for Heuristics on page 1006](#)
- [Examples: Configuring Application Identification Properties on page 1010](#)

## Tracing APPID Operations

---

Tracing operations track all adaptive services operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

By default, no events are traced. If you include the **traceoptions** statement at the **[edit services application-identification]** hierarchy level, the default tracing behavior is as follows:

- Important events are logged in a file called **serviced** located in the **/var/log** directory.
- When the file **serviced** reaches 128 kilobytes (KB), it is renamed **serviced.0**, then **serviced.1**, and so on, until there are three trace files. Then the oldest trace file (**serviced.2**) is overwritten. (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)
- Only the user who configures the tracing operation can access the log files.
- To display the end of the log, issue the **show log serviced | last** operational mode command:

```
[edit]
user@host# run show log serviced | last
```

You cannot change the directory (**/var/log**) in which trace files are located. However, you can customize the other trace file settings by including the following statements:

```
file filename <files number> <match regex> <size size> <(world-readable |
no-world-readable)>;
flag {
  all;
}
```

You configure these statements at the **[edit services application-identification traceoptions]** hierarchy level.

These statements are described in the following sections:

- [Configuring the APPID Log Filename on page 1008](#)
- [Configuring the Number and Size of APPID Log Files on page 1009](#)
- [Configuring Access to the Log File on page 1009](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 1009](#)
- [Configuring the Tracing Flags on page 1009](#)

### Configuring the APPID Log Filename

By default, the name of the file that records trace output is **serviced**. You can specify a different name by including the **file** statement at the **[edit services application-identification traceoptions]** hierarchy level:

```
file filename;
```

## Configuring the Number and Size of APPID Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed *filename.0*, then *filename.1*, and so on, until there are three trace files. Then the oldest trace file (*filename.2*) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit services application-identification traceoptions]** hierarchy level:

```
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (*filename*) reaches 2 MB, *filename* is renamed *filename.0*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0* is renamed *filename.1* and *filename* is renamed *filename.0*. This process repeats until there are 20 trace files. Then the oldest file (*filename.19*) is overwritten by the newest file (*filename.0*).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

## Configuring Access to the Log File

By default, only the user who configures the tracing operation can access log files.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit services application-identification traceoptions]** hierarchy level:

```
file world-readable;
```

To explicitly set the default behavior, include the **file no-world-readable** statement at the **[edit services application-identification traceoptions]** hierarchy level:

```
file no-world-readable;
```

## Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including the **match** statement at the **[edit services application-identification traceoptions file filename]** hierarchy level and specifying a regular expression (regex) to be matched:

```
file filename match regex;
```

## Configuring the Tracing Flags

By default, if the **traceoptions** configuration is present, only important events are logged. You can configure the trace operations to be logged by including the following statements at the **[edit services application-identification traceoptions]** hierarchy level:

```
flag {
  all;
}
```

Currently, the only supported flag is **all**, which instructs the router to trace all operations.

**Related  
Documentation**

- [APPID Overview on page 982](#)
- [Defining an Application Identification on page 995](#)
- [Examples: Configuring Application Identification Properties on page 1010](#)

---

## Examples: Configuring Application Identification Properties

---

The following examples show an address-based application identification configuration:

```
[edit services application-identification]
rule rule1 {
  application-name test2;
  address 1 {
    source {
      ip 10.110.1.1/16;
      port-range {
        tcp 1110-1150;
      }
    }
    destination {
      ip 10.11.1.1/16;
      port-range {
        tcp 111-1100;
      }
    }
    order 1;
  }
}
```

```
[edit services application-identification]
rule-set rs1 {
  rule rule1;
}
profile pf1 {
  rule-set rs1;
}
[edit services]
service-set sset1 {
  application-identification-profile pf1;
}
```

The following examples show application group configuration:

```
[edit services application-identification]
application-group junos:peer-to-peer {
  index 5;
  application-groups {
    junos:chat;
    junos:file-sharing;
    junos:voip;
  }
}
```

```
[edit services application-identification]
application-group junos:voip {
  index 14;
  applications {
    junos:h225ras;
    junos:h225sgn;
    junos:mgcp;
    junos:sip;
  }
}
```

The following examples show application identification for nested application configuration:

```
nested-application nested1 {
  type nested1;
  index 65345;
  protocol HTTP;
  signature nestedcust001 {
    member m01 {
      context http-url-parsed;
      pattern .*nested.*;
      direction any;
    }
    maximum-transactions 2;
    order 3825;
  }
}
```



## CHAPTER 41

# Summary of Application Identification Configuration Statements

The following sections explain each of the application identification configuration statements. The statements are organized alphabetically.

- [address on page 1015](#)
- [application-group on page 1017](#)
- [application-groups \(Services Application Identification\) on page 1018](#)
- [application-system-cache-timeout on page 1018](#)
- [applications \(Services Application Identification\) on page 1019](#)
- [automatic on page 1019](#)
- [bypass-traffic-on-pic-failure on page 1020](#)
- [chain-order on page 1020](#)
- [context on page 1021](#)
- [destination \(Services\) on page 1021](#)
- [direction on page 1022](#)
- [disable-global-timeout-override on page 1024](#)
- [download on page 1025](#)
- [enable-heuristics on page 1025](#)
- [enable-asymmetric-traffic-processing on page 1026](#)
- [enable-heuristics on page 1026](#)
- [idle-timeout on page 1027](#)
- [ignore-errors on page 1027](#)
- [inactivity-non-tcp-timeout on page 1028](#)
- [inactivity-tcp-timeout on page 1028](#)
- [index \(Nested Applications\) on page 1029](#)
- [index on page 1029](#)
- [ip on page 1030](#)
- [max-checked-bytes on page 1030](#)

- [maximum-transactions on page 1031](#)
- [member on page 1031](#)
- [min-checked-bytes on page 1032](#)
- [nested-application on page 1033](#)
- [nested-application-settings on page 1034](#)
- [no-application-identification on page 1034](#)
- [no-application-system-cache on page 1035](#)
- [no-clear-application-system-cache on page 1035](#)
- [no-nested-application on page 1036](#)
- [no-protocol-method on page 1036](#)
- [no-signature-based on page 1037](#)
- [order \(Services Application Identification\) on page 1037](#)
- [pattern on page 1038](#)
- [port-mapping on page 1038](#)
- [port-range on page 1039](#)
- [profile on page 1039](#)
- [protocol on page 1040](#)
- [rule-set \(Services Application Identification\) on page 1047](#)
- [service-set \(Services\) on page 1048](#)
- [service-set-options on page 1050](#)
- [services \(Application Identification\) on page 1050](#)
- [signature on page 1052](#)
- [signature-method-all-ports on page 1052](#)
- [source on page 1053](#)
- [support-uni-directional-traffic on page 1053](#)
- [traceoptions \(Application Identification\) on page 1054](#)
- [type on page 1055](#)
- [type-of-service on page 1055](#)
- [url on page 1056](#)

## address

```
Syntax  address address-name {
          destination {
            ip address</prefix-length>;
            port-range {
              tcp [ ports-and-port-ranges ];
              udp [ ports-and-port-ranges ];
            }
          }
          source {
            ip address</prefix-length>;
            port-range {
              tcp [ ports-and-port-ranges ];
              udp [ ports-and-port-ranges ];
            }
          }
          order number;
        }
```

**Hierarchy Level** [edit services application-identification **rule** *rule-name*]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Define address properties for application-identification rule processing. This statement is mandatory; you must specify either the destination or source properties.

**Options** *address-name*—Identifier for address information.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring APPID Rules on page 997](#)

## application

---

See the following sections:

- [application \(Defining\)](#) on page 1016
- [application \(Including in Rule\)](#) on page 1017

### application (Defining)

**Syntax**

```
application application-name {  
    disable;  
    idle-timeout seconds;  
    index number;  
    port-mapping {  
        disable;  
        port-range {  
            tcp [ ports-and-port-ranges ];  
            udp [ ports-and-port-ranges ];  
        }  
    }  
    session-timeout seconds;  
    type type;  
    type-of-service service-type;  
}
```

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Define the application and its properties.

The remaining statements are explained separately.

**Options** *application-name*—Identifier for the application. This is a mandatory value and has a maximum length of 32 characters.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Defining an Application Identification](#) on page 995

## application (Including in Rule)

<b>Syntax</b>	<code>application <i>application-name</i>;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">rule rule-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Identify the application for inclusion in a rule.
<b>Options</b>	<i>application-name</i> —Identifier for the application.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring APPID Rules on page 997</a></li> </ul>

## application-group

<b>Syntax</b>	<pre> application-group <i>group-name</i> {     disable;     application-groups {         <i>application-group-name</i>;     }     applications {         <i>application-name</i>;     }     index <i>number</i>; } </pre>
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define the properties and contents of the application group.
<b>Options</b>	<p><i>group-name</i>—Unique identifier for the group.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Application Groups on page 1001</a></li> </ul>

## application-groups (Services Application Identification)

---

<b>Syntax</b>	<code>application-groups {     <i>application-group-name</i>; }</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">application-group group-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Identify the list of application groups for inclusion in a larger application group. An <i>application-group-name</i> statement is mandatory.
<b>Options</b>	<i>application-group-name</i> —Identifier for the application group. Maximum length is 32 characters.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Application Groups on page 1001</a></li></ul>

## application-system-cache-timeout

---

<b>Syntax</b>	<code>application-system-cache-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure the lifetime for entries in the application system cache.
<b>Options</b>	<i>seconds</i> — Lifetime for system cache entries, in seconds.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Global APPID Properties on page 1004</a></li></ul>

## applications (Services Application Identification)

---

<b>Syntax</b>	<code>applications {     <i>application-name</i>; }</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">application-group group-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Identify the list of applications for inclusion in the application group.
<b>Options</b>	<i>application-name</i> —Identifier for the application. Maximum length is 32 characters.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Application Groups on page 1001</a></li> </ul>

## automatic

---

<b>Syntax</b>	<code>automatic {     interval <i>hour</i>;     start-time <i>time</i>; }</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">download</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define automatic download properties.
<b>Options</b>	<p><i>interval hour</i>—Download interval in hours. The default is <b>24</b> and the range is from 1 through 168.</p> <p><i>start-time time</i>—Start-time value. The default is <b>0:00</b> and the range is from 0:00 through 24:00.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Automatic Download of Application Package Updates on page 1005</a></li> </ul>

## bypass-traffic-on-pic-failure

---

<b>Syntax</b>	bypass-traffic-on-pic-failure;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> service-set <i>service-set-name</i> service-set-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	<p>When the MultiServices PIC configured for a service set is either administratively taken offline or undergoes a failure, all the traffic entering the configured interface with an IDP service set would be dropped without notification. To avoid this traffic loss, include the <b>bypass-traffic-on-pic-failure</b> statement. When this statement is configured, the affected packets are forwarded in the event of a MultiServices PIC failure or offlining, as though interface-style services were not configured.</p> <p>This issue applies only to Junos Application Aware (previously known as Dynamic Application Awareness) configurations with IDP service sets.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li></ul>

## chain-order

---

<b>Syntax</b>	chain-order;
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application name</a> <a href="#">signature name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Signatures can contain multiple members. If the chain order feature is on, those members are read in order. By default, chain ordering is turned off. If a signature contains only one member, this option is ignored.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li></ul>

## context

---

<b>Syntax</b>	context (http-header-content-type   http-header-host   http-url-parsed   http-url-parsed-param-parsed);
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application name</a> <a href="#">signature name</a> <a href="#">member name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Define a service-specific context, such as <b>http-url</b> .
<b>Options</b>	<b>value</b> —Service-specific context.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li> </ul>

## destination (Services)

---

<b>Syntax</b>	<pre>destination {   ip address &lt;/prefix-length&gt;;   port-range {     tcp [ ports-and-port-ranges ];     udp [ ports-and-port-ranges ];   } }</pre>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">rule rule-name</a> <a href="#">address address-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define destination properties for application-identification rule processing.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring APPID Rules on page 997</a></li> </ul>

## direction

---

<b>Syntax</b>	<code>direction (any   client-to-server   server-to-client) ;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application name</a> <a href="#">signature name</a> <a href="#">member name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the connection direction of the packets to apply pattern matching.
<b>Options</b>	<i>direction</i> —The directions of packets are <b>client-to-server</b> , <b>server-to-client</b> , or <b>any</b> .
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Application Identification for Nested Applications on page 1002</a>.</li></ul>

## disable

---

See the following sections:

- [disable \(APPID Application\) on page 1023](#)
- [disable \(APPID Application Group\) on page 1023](#)
- [disable \(APPID Port Mapping\) on page 1024](#)

### disable (APPID Application)

<b>Syntax</b>	disable;
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">application</a> <i>application-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Disable this application definition.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Defining an Application Identification on page 995</a></li> </ul>

### disable (APPID Application Group)

<b>Syntax</b>	disable;
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">application-group</a> <i>group-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Disable application group properties.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Application Groups on page 1001</a></li> </ul>

## disable (APPID Port Mapping)

<b>Syntax</b>	disable;
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">application</a> <i>application-name</i> <a href="#">port-mapping</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Disable port-mapping properties for application identification.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Defining an Application Identification on page 995</a></li></ul>

---

## disable-global-timeout-override

<b>Syntax</b>	disable-global-timeout-override;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Disallow overriding a global inactivity or session timeout.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Defining an Application Identification on page 995</a></li></ul>

## download

---

<b>Syntax</b>	<pre>download {   automatic {     interval <i>hour</i>;     start-time <i>time</i>;   }   url <i>url</i>; }</pre>
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define application download properties.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Automatic Download of Application Package Updates on page 1005</a></li> </ul>

## enable-heuristics

---

<b>Syntax</b>	enable-heuristics;
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Enables APPID to identify encrypted data packets in point-to-point applications by using heuristics methodology.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring APPID Support for Heuristics on page 1006</a></li> </ul>

## enable-asymmetric-traffic-processing

---

<b>Syntax</b>	enable-asymmetric-traffic-processing;
<b>Hierarchy Level</b>	[edit services service-set <i>service-set-name</i> service-set-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Enables APPID to perform application matching on unidirectional traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring APPID Support for Unidirectional Traffic on page 1007</a></li></ul>

## enable-heuristics


---

<b>Syntax</b>	enable-heuristics;
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Enables APPID to identify encrypted data packets in point-to-point applications by using heuristics methodology.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring APPID Support for Heuristics on page 1006</a></li></ul>

## idle-timeout

<b>Syntax</b>	<code>idle-timeout seconds;</code>
<b>Hierarchy Level</b>	[edit services application-identification <b>application</b> <i>application-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define idle timeout for an application in seconds. When the timeout period expires, the session ends if no packets have been received.
<b>Options</b>	<p><b>seconds</b>—Idle timeout period.</p> <p><b>Default:</b> 30</p> <p><b>Range:</b> 1 through 604,800</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">APPID Overview on page 982</a></li> <li>• <a href="#">Defining an Application Identification on page 995</a></li> </ul>

## ignore-errors

<b>Syntax</b>	<code>ignore-errors &lt;alg&gt; &lt;tcp&gt;;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>services-options</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Define settings for minimizing TCP packet drops during stateful firewall processing.
<div style="display: flex; align-items: center;">  <p><b>NOTE:</b> <code>ignore-errors</code> option is not supported on adaptive services interfaces (<code>sp-x/y/z</code>).</p> </div>	
<b>Options</b>	<p><b>alg</b>—Mediate ALG behavior that results in dropping malformed packets or random packets when the software is unable to allocate resources.</p> <p><b>tcp</b>—Prevent software from dropping packets that fail TCP SYN checks.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Defining an Application Identification on page 995</a></li> </ul>

## inactivity-non-tcp-timeout

---

<b>Syntax</b>	<code>inactivity-non-tcp-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Define the inactivity timeout period for non-TCP established sessions in seconds.
<b>Options</b>	<b><i>seconds</i></b> —Timeout period. <b>Range:</b> 4 through 86,400
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Defining an Application Identification on page 995</a></li></ul>

## inactivity-tcp-timeout

---

<b>Syntax</b>	<code>inactivity-tcp-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Define the inactivity timeout period for TCP established sessions in seconds.
<b>Options</b>	<b><i>seconds</i></b> —Timeout period. <b>Range:</b> 4 through 86,400
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Defining an Application Identification on page 995</a></li></ul>

## index (Nested Applications)

---

<b>Syntax</b>	<code>index number;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Set a number that is a one-to-one mapping to the application name. The application name is used to ensure that each signature definition is unique.
<b>Options</b>	<i>number</i> —Numeric value associated with an application name. The index range for predefined applications is from 1 through 32767. The index range for custom applications and custom nested applications is from 32768 through 65534.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Application Identification for Nested Applications on page 1002</a>.</li> </ul>

## index

---

<b>Syntax</b>	<code>index number;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">application application-name</a> ], [edit services application-identification <a href="#">application-group group-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Assign an application or application-group index number. This is a mandatory value.
<b>Options</b>	<i>number</i> —Index number; must be a unique, unsigned value. <b>Range:</b> 0 through 65535
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Defining an Application Identification on page 995</a></li> <li>• <a href="#">Configuring Application Groups on page 1001</a></li> </ul>

## ip

---

<b>Syntax</b>	<code>ip address&lt;/prefix-length&gt;;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">rule rule-name address destination</a> ], [edit services application-identification <a href="#">rule rule-name address source</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define an IP address and netmask for identifying the traffic destination or source.
<b>Options</b>	<code>address&lt;/prefix-length&gt;</code> —IP address and netmask.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring APPID Rules on page 997</a></li></ul>

## max-checked-bytes

---

<b>Syntax</b>	<code>max-checked-bytes bytes;</code>
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the maximum number of bytes to be inspected.
<b>Options</b>	<code>bytes</code> —Maximum number of bytes. <b>Range:</b> 0 through 100,000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Global APPID Properties on page 1004</a></li></ul>

## maximum-transactions

---

<b>Syntax</b>	<code>maximum-transactions <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application name</a> <a href="#">signature name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Set the maximum number of transactions required before a match is made.
<b>Options</b>	<i>number</i> —Maximum number of transactions.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li></ul>

## member

---

<b>Syntax</b>	<code>member <i>name</i>;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application name</a> <a href="#">signature name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Define a member name for a custom nested application signature definition. Custom definitions can contain multiple members that define attributes for an application.
<b>Options</b>	<i>name</i> —Name of member for a custom nested application signature definition.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li></ul>

## min-checked-bytes

---

<b>Syntax</b>	min-checked-bytes <i>bytes</i> ;
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the minimum number of bytes to be inspected.
<b>Options</b>	<i>bytes</i> —Minimum number of bytes. <b>Range:</b> 0 through 2000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Global APPID Properties on page 1004</a></li></ul>

## nested-application

<b>Syntax</b>	<pre> nested-application <i>name</i> {   <i>index</i> <i>number</i>;   <i>protocol</i> <i>protocol</i> ;   <i>signature</i> <i>name</i> {     <i>chain-order</i> ;     <i>maximum-transactions</i> <i>number</i>;     <i>member</i> <i>name</i> {       <i>context</i> (http-header-content-type   http-header-host   http-url-parsed           http-url-parsed-param-parsed);       <i>direction</i> (any   client-to-server   server-to-client);       <i>pattern</i> <i>dfa-pattern</i>;     }     <i>order</i> <i>number</i>;   }   <i>type</i> <i>type</i>; } </pre>
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure a custom nested application definition for the desired application name that will be used by the system to identify the nested application as it passes through the device. Custom nested application definitions can be used for nested applications that are not part of the Juniper Networks predefined nested application database.
<b>Options</b>	<p><i>name</i>—Name of nested application.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li> </ul>

## nested-application-settings

---

<b>Syntax</b>	nested-application-settings { no-application-system-cache; no-nested-application; }
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure nested application options for application identification services.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Application Identification for Nested Applications on page 1002.</a></li></ul>

## no-application-identification

---

<b>Syntax</b>	no-application-identification;
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Disable all application identification methods.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Global APPID Properties on page 1004</a></li></ul>

## no-application-system-cache

---

<b>Syntax</b>	no-application-system-cache;
<b>Hierarchy Level</b>	[edit services application-identification], [edit services application-identification <a href="#">nested-application-settings</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Disable storing application identification results in the application system cache. Nested application identification information is saved in the application system cache to improve performance. This cache is updated when a different application is identified. This caching is turned on by default. Use the no-application-system-cache statement to turn it off.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Global APPID Properties on page 1004</a></li><li>• <a href="#">Application Identification for Nested Applications on page 1002</a>.</li></ul>

## no-clear-application-system-cache

---

<b>Syntax</b>	no-clear-application-system-cache;
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Disable clearing the application system cache.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Global APPID Properties on page 1004</a></li></ul>

## no-nested-application

---

<b>Syntax</b>	no-nested-application;
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application-settings</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Sometimes there is a need to identify multiple different applications running on the same Layer 7 protocols. For example, both Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications. To do this, the application layer is split into two layers: Layer 7 applications and Layer 7 protocols. This function is turned on by default. Use the <b>no-nested-application</b> statement to turn it off.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li></ul>

## no-protocol-method

---

<b>Syntax</b>	no-protocol-method;
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Disable the protocol-based application identification method.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Global APPID Properties on page 1004</a></li></ul>

## no-signature-based

---

<b>Syntax</b>	no-signature-based;
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Disable the signature-based application identification method.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Global APPID Properties on page 1004</a></li> </ul>

## order (Services Application Identification)

---

<b>Syntax</b>	order <i>number</i> ;
<b>Hierarchy Level</b>	[edit services application-identification <i>nested-application name signature name member name</i> ] [edit services application-identification <i>rule rule-name address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define application matching priority. For address configurations, the order number resolves the conflict when multiple address entries are matched for a specific session. The lower number has higher priority.
<b>Options</b>	<i>number</i> —Order number. This value is mandatory and must be unique.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring APPID Rules on page 997</a></li> <li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li> </ul>

## pattern

---

<b>Syntax</b>	<code>pattern <i>dfa-pattern</i>;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application name</a> <a href="#">signature name</a> <a href="#">member name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Define an attack pattern to be detected.
<b>Options</b>	<i>dfa-pattern</i> —Pattern of attack to match. Deterministic Finite Automata (DFA) is a powerful pattern matching engine.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li></ul>

## port-mapping

---

<b>Syntax</b>	<pre>port-mapping {   <a href="#">disable</a>;   <a href="#">port-range</a> {     tcp [ <i>ports-and-port-ranges</i> ];     udp [ <i>ports-and-port-ranges</i> ];   } }</pre>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">application application-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define port-mapping properties for application identification.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Defining an Application Identification on page 995</a></li></ul>

## port-range

<b>Syntax</b>	<pre>port-range {     tcp [ <i>ports-and-port-ranges</i> ];     udp [ <i>ports-and-port-ranges</i> ]; }</pre>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">application</a> <i>application-name</i> <a href="#">port-mapping</a> ], [edit services application-identification <a href="#">rule</a> <i>rule-name</i> <a href="#">address destination</a> ], [edit services application-identification <a href="#">rule</a> <i>rule-name</i> <a href="#">address source</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define TCP and UDP port numbers or numeric ranges. For port-mapping configurations, this entry is required if the parent node exists.
<b>Options</b>	<b><i>ports-and-port-ranges</i></b> —Individual port numbers, numeric port ranges, or both. Separate the values with spaces. The format for numeric port ranges is <i>minimum-value–maximum-value</i> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Defining an Application Identification on page 995</a></li> <li>• <a href="#">Configuring APPID Rules on page 997</a></li> </ul>

## profile

<b>Syntax</b>	<pre>profile <i>profile-name</i> {     <a href="#">rule-set</a> <i>rule-set-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define members of application profile, which consists of one or more rule sets.
<b>Options</b>	<b><i>profile-name</i></b> —Identifier for application profile.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Application Profiles on page 1001</a></li> </ul>

## protocol

---

<b>Syntax</b>	<code>protocol <i>protocol</i>;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Identify the protocol that will be monitored to identify nested applications. HTTP is supported.
<b>Options</b>	<i>protocol</i> —An agreed-upon or standardized method for transmitting data and establishing communications between different devices. The value <b>http</b> is supported.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li></ul>

## hcm

---

See the following sections:

- [from](#) on page 1041
- [host](#) on page 1042
- [request-url](#) on page 1042
- [term](#) on page 1043
- [then](#) on page 1043
- [url](#) on page 1044
- [url-list](#) on page 1044
- [url-rule](#) on page 1045
- [url-rule-set](#) on page 1045

## from

**Syntax**    from {  
                   url-list *url-list-name*;  
                   url *url\_identifier* {  
                     host *hostname*;  
                     request-url *page-name*;  
                   }  
                 }

**Hierarchy Level**    [edit services hcm url-rule *url-rule-name* term *term-num*]

**Release Information**    Statement introduced in Junos OS Release 12.1.

**Description**    Specify input conditions for the HCM term.

**Options**    The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                       interface-control—To add this statement to the configuration.

## host

<b>Syntax</b>	host <i>hostname</i> ;
<b>Hierarchy Level</b>	[edit services hcm url-rule <i>url-rule-name</i> term <i>term-num</i> from url <i>url_identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Specify a hostname for the matching URL for the <b>term</b> . A match for that term is considered when a URL matches the <b>hostname</b> and the <b>request-URL</b> within the same term.
<b>Options</b>	<b>hostname</b> —Name of the host for the URL rule.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## request-url

<b>Syntax</b>	request-url <i>page-name</i> ;
<b>Hierarchy Level</b>	[edit services hcm url-rule <i>url-rule-name</i> term <i>term-num</i> from url <i>url_identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Specify a request-URL to match the <b>term</b> . A match for the term is considered when a URL matches any hostname and any request-URL within a term.
<b>Options</b>	<b>page-name</b> —Page name of the request URL.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

**term**

<b>Syntax</b>	<pre> term <i>term-num</i> {   from {     url-list <i>url-list-name</i>;     url <i>url_identifier</i> {       host <i>hostname</i>;       request-url <i>page-name</i>;     }   } } </pre>
<b>Hierarchy Level</b>	[edit services hcm url-rule <i>url-rule-name</i> term <i>term-num</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Specify a numbered identity for each term inside a rule.
<b>Options</b>	<p><b><i>term-num</i></b>—Identifier value for the term.</p> <p><b>Range:</b> 1 through 255</p> <p><b>Default:</b> If no value is entered, the default value is 1.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

**then**

<b>Syntax</b>	<pre> then {   discard;   accept;   count;   log-request; } </pre>
<b>Hierarchy Level</b>	[edit services hcm url-rule <i>url-rule-name</i> term <i>term-num</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Define the HCM term actions.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

## url

<b>Syntax</b>	<code>url <i>url_identifier</i>;</code>
<b>Hierarchy Level</b>	[edit services hcm url-rule <i>url-rule-name</i> term <i>term-num</i> from]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Specify an integer that uniquely identifies a particular URL definition within a term.
<b>Options</b>	<i>url_identifier</i> —URL identifier number. <b>Range:</b> 1 through 32,767 <b>Default:</b> If no value is added, the default value is 1.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## url-list

<b>Syntax</b>	<code>url-list <i>url-list-name</i> ;</code>
<b>Hierarchy Level</b>	[edit services hcm url-rule <i>url-rule-name</i> term <i>term-num</i> from]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1.
<b>Description</b>	Specify the name of a previously defined URL list to be included as a matching condition. A match for the term is considered when a URL matches any hostname and any request-URL within the same term.
<b>Options</b>	<i>url-list-name</i> —Name of the previously defined URL list.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## url-rule

**Syntax**

```
url-rule url-rule-name {
  term term-num {
    from {
      url-list url-list-name;
      url url_identifier {
        host hostname;
        request-url page-name;
      }
    }
    then {
      discard;
      accept;
      count;
      log-request;
    }
  }
}
```

**Hierarchy Level** [edit services hcm]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** Specify the name of the URL rule.

**Options** *url-rule-name*—Name of the URL rule.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

## url-rule-set

**Syntax**

```
url-rule-set url-rule-set-name {
  url-rule rule1;
  url-rule rule2;
}
```

**Hierarchy Level** [edit services hcm url-rule *url-rule-name*]

**Release Information** Statement introduced in Junos OS Release 11.2.

**Description** Specify the name of the rule set. A rule set is a collection of rules ordered in the sequence in which they are entered.

**Options** *url-rule-set-name*—Name of the collection of URL rules that constitute this rule set.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

## rule

See the following sections:

- [rule \(Configuring\) on page 1046](#)
- [rule \(Including in Rule Set\) on page 1047](#)

### rule (Configuring)

```
Syntax  rule rule-name {
        address {
            destination {
                ip address </prefix-length>;
                port-range {
                    tcp [ ports-and-port-ranges ];
                    udp [ ports-and-port-ranges ];
                }
            }
            source {
                ip address </prefix-length>;
                port-range {
                    tcp [ ports-and-port-ranges ];
                    udp [ ports-and-port-ranges ];
                }
            }
            order number;
        }
        application application-name;
    }
```

**Hierarchy Level** [edit services application-identification]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Define properties for application-identification rule processing.

**Options** *rule-name*—Unique identifier for the rule.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring APPID Rules on page 997](#)

## rule (Including in Rule Set)

<b>Syntax</b>	<code>rule <i>rule-name</i>;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">rule-set</a> <i>rule-set-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Identify rules for inclusion in application rule set.
<b>Options</b>	<i>rule-name</i> —Unique identifier for the rule.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring APPID Rules on page 997</a></li></ul>

## rule-set (Services Application Identification)

---

<b>Syntax</b>	<code>rule-set <i>rule-set-name</i> {     <a href="#">rule</a> <i>application-rule-name</i>; }</code>
<b>Hierarchy Level</b>	[edit services application-identification], [edit services application-identification <a href="#">profile</a> <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define members of rule set.
<b>Options</b>	<i>rule-set-name</i> —Unique identifier for the rule set.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring APPID Rules on page 997</a></li></ul>

## service-set (Services)

```
Syntax  service-set service-set-name {
        allow-multicast;
        extension-service service-name {
            provider-specific-rules-configuration;
        }
        (ids-rules rule-name | ids-rule-sets rule-set-name);
        interface-service {
            service-interface interface-name;
        }
        ipsec-vpn-options {
            anti-replay-window-size bits;
            clear-dont-fragment-bit;
            ike-access-profile profile-name;
            local-gateway address;
            no-anti-replay;
            passive-mode-tunneling;
            trusted-ca [ ca-profile-names ];
            tunnel-mtu bytes;
        }
        ip-reassembly-rules rule-name;
        (ipsec-vpn-rules rule-name | ipsec-vpn-rule-sets rule-set-name);
        max-flows number;
        max-drop-flows {
            ingress ingress-flows;
            egress egress-flows;
        }
        nat-options {
            land-attack-check (ip-only | ip-port);
            max-sessions-per-subscriber session-number;
            stateful-nat64 {
                clear-dont-fragment-bit;
            }
        }
        (nat-rules rule-name | nat-rule-sets rule-set-name);
        next-hop-service {
            inside-service-interface interface-name.unit-number;
            outside-service-interface interface-name.unit-number;
            outside-service-interface-type local;
            service-interface-pool name;
        }
        (pgcp-rules rule-name | pgcp-rule-sets rule-set-name);
        (ptsp-rules rule-name | ptsp-rule-sets rule-set-name);
        service-set-options {
            bypass-traffic-on-exceeding-flow-limits;
            bypass-traffic-on-pic-failure;
            enable-asymmetric-traffic-processing;
            support-uni-directional-traffic;
        }
        snmp-trap-thresholds {
            flows high high-threshold | low low-threshold;
            nat-address-port high-threshold | low low-threshold;
        }
    }
```

```

}
software-options {
    dslite-ipv6-prefix-length dslite-ipv6-prefix-length;
}
(software-rules rule-name | software-rule-sets rule-set-name);
(stateful-firewall-rules rule-name | stateful-firewall-rule-sets rule-set-name);
syslog {
    host hostname {
        class {
            alg-logs;
            ids-logs;
            nat-logs;
            packet-logs;
            pcp-logs;
            session-logs <open | close>;
            stateful-firewall-logs ;
        }
        services severity-level;
        facility-override facility-name;
        interface-service prefix-value;
    }
}
}

```

Hierarchy Level	[edit services]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p><b>pgcp-rules</b> and <b>pgcp-rule-sets</b> options added in Junos OS Release 8.4.</p> <p><b>server-set-options</b> option added in Junos OS Release 10.1.</p> <p><b>ptsp-rules</b> and <b>ptsp-rule-sets</b> options added in Junos OS Release 10.2.</p> <p><b>software-rules</b> and <b>clear-rule-sets</b> options added in Junos OS Release 10.4.</p> <p><b>software-options</b> option added in Junos OS Release 14.1.</p>
Description	Define the service set.
Options	<p><b><i>service-set-name</i></b>—Name of the service set.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <li><i>Service Set Properties</i></li> </ul>

## service-set-options

---

Syntax	<pre>service-set-options {     bypass-traffic-on-exceeding-flow-limits;     bypass-traffic-on-pic-failure;     enable-asymmetric-traffic-processing;     support-uni-directional-traffic;     header-integrity-check }</pre>
Hierarchy Level	[edit services service-set]
Release Information	Statement introduced in Junos OS Release 10.1. The <b>enable-asymmetric-traffic-processing</b> and the <b>support-uni-directional-traffic</b> options were added in Release 11.2.
Description	Specify the service set options to apply to a service set.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Service Sets to be Applied to Services Interfaces on page 742</a></li><li>• <a href="#">Configuring APPID Support for Unidirectional Traffic on page 1007</a></li></ul>

## services (Application Identification)

---

Syntax	<pre>services application-identification { ... }</pre>
Hierarchy Level	[edit]
Release Information	<b>services</b> statement introduced before Junos OS Release 7.4. <b>application-identification</b> statement introduced in Junos OS Release 9.5.
Description	Define the services to be applied to traffic.
Options	<b>application-identification</b> —The values configured for application-identification properties.  The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Application Identification</i></li></ul>

## session-timeout

---

See the following sections:

- [session-timeout \(Interfaces\) on page 1051](#)
- [session-timeout \(Application Identification\) on page 1051](#)

### session-timeout (Interfaces)

<b>Syntax</b>	<code>session-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">services-options</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Define session lifetime globally for the Multiservices interface in seconds.
<b>Options</b>	<i>seconds</i> —Duration of session. <b>Range:</b> 4 through 86,400
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Defining an Application Identification on page 995</a></li> </ul>

### session-timeout (Application Identification)

<b>Syntax</b>	<code>session-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">application</a> <i>application-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define session lifetime for the specified application in seconds.
<b>Options</b>	<i>seconds</i> —Duration of session. <b>Default:</b> 3600 <b>Range:</b> 1 through 604,800
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Defining an Application Identification on page 995</a></li> </ul>

## signature

---

<b>Syntax</b>	<pre>signature <i>name</i> {   chain-order;   maximum-transactions <i>number</i>;   member <i>name</i> {     context <i>value</i>;     direction (any   client-to-server   server-to-client);     pattern <i>dfa-pattern</i>;   }   order <i>number</i>; }</pre>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">nested-application name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Identify the name of the custom nested application signature definition. The name must be unique with a maximum length of 32 characters.
<b>Options</b>	<i>name</i> —Name of the signature definition.  The remaining statements are described separately.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Application Identification for Nested Applications on page 1002</a></li></ul>

## signature-method-all-ports

---

<b>Syntax</b>	signature-method-all-ports
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	<p>Runs signature matching on all traffic in application-identification. This is called the signature-match mode.</p> <p>In the default mode, or fast-port-match mode, all traffic destined to well-known ports (up to 1024) immediately returns the final port match. However, the device runs signature matching for all traffic destined for port 80,</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Global APPID Properties on page 1004</a></li></ul>

## source

<b>Syntax</b>	<pre>source {   ip address &lt;/prefix-length&gt;;   port-range {     tcp [ ports-and-port-ranges ];     udp [ ports-and-port-ranges ];   } }</pre>
<b>Hierarchy Level</b>	[edit services application-identification <b>rule</b> <i>rule-name</i> <b>address</b> <i>address-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define source properties for application-identification rule processing.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring APPID Rules on page 997</a></li> </ul>

## support-uni-directional-traffic

<b>Syntax</b>	support-uni-directional-traffic;
<b>Hierarchy Level</b>	[edit services service-set <i>service-set-name</i> service-set-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Enables APPID to perform application matching on unidirectional traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring APPID Support for Unidirectional Traffic on page 1007</a></li> </ul>

## traceoptions (Application Identification)

---

<b>Syntax</b>	<pre>traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regex</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable           no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace; }</pre>
<b>Hierarchy Level</b>	[edit services application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	<p>Configure application identification tracing options.</p> <p>To specify more than one tracing operation, include multiple <b>flag</b> statements.</p>
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b><i>trace-file</i></b> reaches its maximum size, it is renamed <b><i>trace-file.0</i></b>, then <b><i>trace-file.1</i></b>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 2 files</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>flag</b>—Tracing operation to perform. <b>all</b> is the only valid completion.</p> <ul style="list-style-type: none"><li>• <b>all</b>—Trace all events.</li></ul> <p><b>match <i>regex</i></b>—(Optional) Regular expression for lines to be logged.</p> <p><b>no-world-readable</b>—(Optional) Disallow any user to read the log file.</p> <p><b>size <i>size</i></b>—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named <b><i>trace-file</i></b> reaches this size, it is renamed <b><i>trace-file.0</i></b>. When the <b><i>trace-file</i></b> again reaches its maximum size, <b><i>trace-file.0</i></b> is renamed <b><i>trace-file.1</i></b> and <b><i>trace-file</i></b> is renamed <b><i>trace-file.0</i></b>. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p><b>Syntax:</b> <b>xk</b> to specify KB, <b>xm</b> to specify MB, or <b>xg</b> to specify GB</p> <p><b>Range:</b> 10240 through 1073741824 or the maximum file size supported on your system</p> <p>If you specify a maximum file size, you also must specify a maximum number of trace files with the <b>files</b> option.</p> <p><b>world-readable</b>—(Optional) Allow any user to read the log file.</p>

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Tracing APPID Operations on page 1008](#)

## type

**Syntax** type *type*;

**Hierarchy Level** [edit services application-identification [application](#) *application-name*]  
[edit services application-identification [nested-application](#) *name*]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Define type of application, such as HTTP or FTP.

**Options** **type**—Application type. This is a mandatory value and has a maximum length of 32 characters.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Defining an Application Identification on page 995](#)
- [Application Identification for Nested Applications on page 1002](#)

## type-of-service

**Syntax** type-of-service *service-type*;

**Hierarchy Level** [edit services application-identification [application](#) *application-name*]

**Release Information** Statement introduced in Junos OS Release 9.5.

**Description** Define the type of service by service objective. There is no default value.

**Options** The following **service-type** options are available:

- **maximize-reliability**—Service designed for maximum reliability in packet transmission.
- **maximize-throughput**—Service designed for maximum throughput.
- **minimize-delay**—Service designed for minimum delay in packet transmission.
- **minimize-monetary-cost**—Service designed for minimum monetary cost.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Defining an Application Identification on page 995](#)

## url

---

<b>Syntax</b>	<code>url url;</code>
<b>Hierarchy Level</b>	[edit services application-identification <a href="#">download</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define the URL for application package downloads.
<b>Options</b>	<code>url</code> —Download URL.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Automatic Download of Application Package Updates on page 1005</a></li></ul>

# Application-Aware Access List Configuration Guidelines

To configure application-aware access list (AACL) services, include the **aac**l statements at the **[edit services]** hierarchy level:

```
[edit services]
aac
```

`l {
 rule rule-name {
 match-direction (input | output | input-output);
 term term-name {
 from {
 application-group-any;
 application-groups [ application-group-names ];
 application-unknown;
 applications [ application-names ];
 destination-address address <any-unicast>;
 destination-address-range low minimum-value high maximum-value;
 destination-prefix-list list-name;
 source-address address <any-unicast>;
 source-address-range low minimum-value high maximum-value;
 source-prefix-list list-name;
 }
 then {
 (accept | discard);
 count (application | application-group | application-group-any | none);
 forwarding-class class-name;
 policer policer-name;
 }
 }
 }
}
rule-set rule-set-name {
 [ rule rule-names ];
}`

This chapter contains the following sections:

- [Configuring AAAC](#) Rules on page 1058
- [Configuring AAAC](#) Rule Sets on page 1062

- [Configuring Logging of ACL Flows on page 1063](#)
- [Example: Configuring ACL Rules on page 1064](#)

## Configuring ACL Rules

---

To configure an ACL rule, include the **rule** *rule-name* statement at the **[edit services aac]** hierarchy level:

```
rule rule-name {
  match-direction (input | output | input-output);
  term term-name {
    from {
      application-group-any;
      application-groups [ application-group-names ];
      applications [ application-names ];
      destination-address address <any-unicast>;
      destination-address-range low minimum-value high maximum-value;
      destination-prefix-list list-name;
      nested-applications [ nested-application-names ];
      nested-application-unknown
      source-address address <any-unicast>;
      source-address-range low minimum-value high maximum-value;
      source-prefix-list list-name;
    }
    then {
      (accept | discard);
      count (application | application-group | application-group-any | nested-application
        | none);
      forwarding-class class-name;
      policer policer-name;
    }
  }
}
```

Each ACL rule consists of a set of terms, similar to a filter configured at the **[edit firewall]** hierarchy level. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software.

The following sections explain how to configure the components of ACL rules:

- [Configuring Match Direction for ACL Rules on page 1059](#)
- [Configuring Match Conditions in ACL Rules on page 1059](#)
- [Configuring Actions in ACL Rules on page 1060](#)
- [Logging ACL Flows Based on Application on page 1061](#)

## Configuring Match Direction for ACL Rules

Each rule must include a **match-direction** statement that specifies the direction in which the rule match is applied. To configure where the match is applied, include the **match-direction** statement at the **[edit services aac rule *rule-name*]** hierarchy level:

```
match-direction (input | output | input-output);
```

If you configure **match-direction input-output**, bidirectional rule creation is allowed.

The match direction is used with respect to the traffic flow through the services PIC or DPC. When a packet is sent to the PIC or DPC, direction information is carried along with it.

With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.

With a next-hop service set, packet direction is determined by the interface used to route the packet to the services PIC or DPC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the PIC or DPC, the packet direction is output. For more information on inside and outside interfaces, see [“Configuring Service Sets to be Applied to Services Interfaces” on page 742](#).

On the PIC or DPC, a flow lookup is performed. If no flow is found, rule processing is performed. All rules in the service set are considered. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that matches the packet direction are considered.

## Configuring Match Conditions in ACL Rules

To configure ACL match conditions, include the **from** statement at the **[edit services aac rule *rule-name* term *term-name*]** hierarchy level:

```
from {
  application-group-any;
  application-groups [ application-group-names ];
  applications [ application-names ];
  destination-address address <any-unicast>;
  destination-address-range low minimum-value high maximum-value;
  destination-prefix-list list-name;
  nested-applications [ nested-application-names ];
  nested-application-unknown
  source-address address <any-unicast>;
  source-address-range low minimum-value high maximum-value;
  source-prefix-list list-name;
}
```

IPv4 and IPv6 source and destination addresses are supported. You can use either the source address or the destination address as a match condition, in the same way that you configure a firewall filter; for more information, see the *Routing Policy Feature Guide for Routing Devices*.

Alternatively, you can specify a list of source or destination prefixes by configuring the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either

the **destination-prefix-list** or the **source-prefix-list** statement in the ACL rule. For an example, see [“Example: Configuring ACL Rules” on page 1064](#).

If you omit the **from** term, the ACL rule accepts all traffic and the default protocol handlers take effect:

- User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP) create a bidirectional flow with a predicted reverse flow.
- IP creates a unidirectional flow.

You can also include application and application group definitions you have configured at the **[edit services application-identification]** hierarchy level; for more information, see the topics in *Application Identification*.

- To apply one or more specific application protocol definitions, include the **applications** statement at the **[edit services aacl rule rule-name term term-name from]** hierarchy level.
- To apply one or more sets of application group definitions you have defined, include the **application-groups** statement at the **[edit services aacl rule rule-name term term-name from]** hierarchy level.



**NOTE:** If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the **[edit services application-identification]** hierarchy level; you cannot specify these properties as match conditions.

- To consider any application group defined in the database as a match, include the **application-group-any** statement at the **[edit services aacl rule rule-name term term-name from]** hierarchy level.
- To consider any nested application defined in the database a match, include the **nested-applications** statement at the **[edit services aacl rule rule-name term term-name from]** hierarchy level. Nested applications are protocols that run on a parent application. For example, if the Facebook application runs on the parent application `junos:http`, the nested application will be `junos:http:facebook`.

## Configuring Actions in ACL Rules

To configure ACL actions, include the **then** statement at the **[edit services aacl rule rule-name term term-name]** hierarchy level:

```
then {
  (accept | discard);
  (count (application | application-group | application-group-any | nested-application |
    none) | forwarding-class class-name);
}
```

You must include one of the following actions:

- **accept**—The packet is accepted and sent on to its destination.
- **discard**—The packet is not accepted and is not processed further.

When you select **accept** as the action, you can optionally configure one or both of the following action modifiers. No action modifiers are allowed with the **discard** action.

- **count (application | application-group | application-group-any | nested-application | none)**—For all accepted packets that match the rules, record a packet count using ACL statistics practices. You can specify one of the following options; there is no default setting:
  - **application**—Count the application that matched in the **from** clause.
  - **application-group**—Count the application group that matched in the **from** clause.
  - **application-group-any**—Count all application groups that match **from application-group-any** under the **any** group name.
  - **nested-application**—Count all nested applications that matched in the **from** clause.
  - **none**—Same as not specifying **count** as an action.



**NOTE:**

- When a session closes before APPID has identified nested applications, the session is treated as a best-effort session and ACL does not get the nested application information. In such cases, nested applications will be reported as unknown applications.
- During the time that the application identification (APPID) feature has not yet made a final determination of the application associated with a given flow, the flow does not contribute to any per-subscriber or per-application statistics collection. For more information, see [“Best-Effort Application Identification of DPI-Serviced Flows” on page 988](#).

- **forwarding-class class-name**—Specify the packets' forwarding-class name.

You can optionally include a **policer** that has been specified at the **[edit firewall]** hierarchy level. Only the bit-rate and burst-size properties specified for the policer are applied in the ACL rule set. The only action application when a policer is configured is **discard**. For more information on policer definitions, see the *Routing Policy Feature Guide for Routing Devices*.

## Logging ACL Flows Based on Application

You can now log ACL flows based on application. You can select a specific application or request information on unknown applications.

You can now configure ACL rules to match unknown applications. All existing actions that can apply to recognized applications can also apply to unknown applications. You can use the following statements at the **[edit services acl rule rule-name term term-name from]** hierarchy level:

- application-group-any
- application-groups
- application-unknown
- applications
- nested-application-unknown
- nested-applications

The addition of matching “application unknown” enables the specific logging of the input flows associated with applications that cannot be identified. Because logging is triggered by an input event, you must specify **match-direction** as **input-output** or **input**.

To configure logging of flows for AACL, include the **match-direction input** or **match-direction input-output** statement at the **[edit services aacl rule *rule-name*]** hierarchy level, include an **applications** or **application-unknown** statement at the **[edit services aacl rule *rule-name* term *term-name* from]** hierarchy level, and include only one **log** statement at the **[edit services aacl rule *rule-name* term *term-name* then]** hierarchy level. The log statements can include any of the following options:

- session-start
- session-end
- session-start-end-no-stats
- session-start-interim-end
- session-interim-end
- session-end

**Related  
Documentation**

- [AACL Overview on page 984](#)
- [Configuring AACL Rule Sets on page 1062](#)
- [Configuring Logging of AACL Flows on page 1063](#)
- [Example: Configuring AACL Rules on page 1064](#)

---

## Configuring AACL Rule Sets

The **rule-set** statement defines a collection of AACL rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the **rule-set** statement at the **[edit services aacl]** hierarchy level with a **rule** statement for each rule:

```
rule-set rule-set-name {  
  rule rule-name;  
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing continues to the next rule in the rule set. If none of the rules matches the packet, the packet is dropped by default.

**Related  
Documentation**

- [AACL Overview on page 984](#)
- [Configuring AACL Rules on page 1058](#)
- [Configuring Logging of AACL Flows on page 1063](#)
- [Example: Configuring AACL Rules on page 1064](#)

## Configuring Logging of AACL Flows

You can configure logging of AACL flows for a given application or for all unknown applications using AACL rules. You must set **match-direction** to **input** or **input-output** for logging to occur.

1. Create a rule and term.

```
user@host# edit services aacl rule rule-name term term-name
```

2. Specify selection of an application.

```
[edit services aacl rule rule-name term term-name]
user@host# set from applications application-name
```

OR

Specify selection of all unknown applications.

```
[edit services aacl rule <variable>rule-name</variable> term
<variable>term-name</variable>]
set from application-unknown
```

3. In the **then** statement, specify logging of input flow.

```
[edit services aacl rule rule-name term term-name]
user@host# set then log input-flows]
```

**Example—Configuration  
of Logging of Input  
Flows for Unknown  
Applications**

```
[edit services aacl rule aacl_rule5]
match-direction input-output;
term t0 {
  from {
    application-unknown;
  }
  then {
    count application;
    log input-flow;
    accept;
  }
}
```

**Example—Setup of a Specific Log File**

The following example shows how to direct the aacL flow log to a file other than the default syslog file on the Routing Engine file system.

```
[edit system syslog]
file aacL_log {
  external any;
  match aacL-flow-log;
}
```

**Related Documentation**

- [AACL Overview on page 984](#)
- [Configuring AACL Rules on page 1058](#)
- [Configuring AACL Rule Sets on page 1062](#)
- [Example: Configuring AACL Rules on page 1064](#)

---

## Example: Configuring AACL Rules

---

The following example shows an AACL configuration containing a rule with three terms using a variety of match conditions and actions:

```
[edit services aacL]
rule aacL-test {
  match-direction input;
  term term1 {
    from {
      source-address 10.0.1.1
      application test1;
    }
    then {
      accept;
    }
  }
  term term2 {
    from {
      source-address {
        any-unicast;
      }
      application test1;
    }
    then {
      discard;
    }
  }
  term term3 {
    from {
      source-address {
        any-unicast;
      }
      application test1 test2;
    }
    then {
      accept;
      count application;
    }
  }
}
```

```
}  
}  
}
```

- Related Documentation**
- [AACL Overview on page 984](#)
  - [Configuring AACL Rules on page 1058](#)



## CHAPTER 43

# Summary of AACL Configuration Statements

The following sections explain each of the application-aware access list (AACL) services statements. The statements are organized alphabetically.

### applications (Services AACL)

---

<b>Syntax</b>	<code>applications [ <i>application-names</i> ];</code>
<b>Hierarchy Level</b>	[edit services aacl <b>rule</b> <i>rule-name</i> <b>term</b> <i>term-name</i> <b>from</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Identify one or more applications defined in the application identification configuration for inclusion as a match condition.
<b>Options</b>	<i>application-names</i> —Identifiers of the applications.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in AACL Rules on page 1059</a></li></ul>

## application-groups (Services ACL)

---

<b>Syntax</b>	<code>application-groups [ <i>application-group-names</i> ];</code>
<b>Hierarchy Level</b>	[edit services aacl <a href="#">rule rule-name</a> <a href="#">term term-name</a> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Identify one or more application groups defined in the application identification configuration for inclusion as a match condition.
<b>Options</b>	<i>application-group-names</i> —Identifiers of the application groups.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in ACL Rules on page 1059</a></li></ul>

## application-group-any

---

<b>Syntax</b>	<code>application-group-any;</code>
<b>Hierarchy Level</b>	[edit services aacl <a href="#">rule rule-name</a> <a href="#">term term-name</a> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Indicates that any application group defined in the database is considered a match.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in ACL Rules on page 1059</a></li></ul>

## application-unknown

---

<b>Syntax</b>	<code>application-unknown</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> aacl <a href="#">rule rule-name</a> <a href="#">term term-name</a> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Enable ACL logging of flows for unknown applications.

## destination-address

---

<b>Syntax</b>	<code>destination-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit services aacl <a href="#">rule rule-name</a> <a href="#">term term-name</a> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the destination address for rule matching.
<b>Options</b>	<i>address</i> —Destination IPv4 or IPv6 address or prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Match Conditions in ACL Rules on page 1059</a></li> </ul>

## destination-address-range

---

<b>Syntax</b>	<code>destination-address-range low <i>minimum-value</i> high <i>maximum-value</i>;</code>
<b>Hierarchy Level</b>	[edit services aacl <a href="#">rule rule-name</a> <a href="#">term term-name</a> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the destination address range for rule matching.
<b>Options</b>	<i>minimum-value</i> —Lower boundary for the IPv4 or IPv6 address range. <i>maximum-value</i> —Upper boundary for the IPv4 or IPv6 address range.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Match Conditions in ACL Rules on page 1059</a></li> </ul>

## destination-prefix-list

---

<b>Syntax</b>	<code>destination-prefix-list <i>list-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services aacl <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i> <a href="#">from</a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the destination prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the <code>[edit policy-options]</code> hierarchy level.
<b>Options</b>	<i>list-name</i> —Destination prefix list.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in AACL Rules on page 1059</a></li></ul>

## from

---

<b>Syntax</b>	<pre>from {   <a href="#">application-group-any</a>;   <a href="#">application-groups</a> [ <i>application-group-names</i> ];   <a href="#">application-unknown</a>;   <a href="#">applications</a> [ <i>application-names</i> ];   <a href="#">destination-address</a> <i>address</i> &lt;any-unicast&gt;;   <a href="#">destination-address-range</a> low <i>minimum-value</i> high <i>maximum-value</i>;   <a href="#">destination-prefix-list</a> <i>list-name</i>;   nested-application-unknown;   <a href="#">source-address</a> <i>address</i> &lt;any-unicast&gt;;   <a href="#">source-address-range</a> low <i>minimum-value</i> high <i>maximum-value</i>;   <a href="#">source-prefix-list</a> <i>list-name</i>; }</pre>
<b>Hierarchy Level</b>	<code>[edit <a href="#">services</a> aacl <a href="#">rule</a> <i>rule-name</i> <a href="#">term</a> <i>term-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 9.5.
<b>Description</b>	Specify match conditions for the AACL term.
<b>Options</b>	For information on match conditions, see the description of firewall filter match conditions in the <i>Routing Policy Feature Guide for Routing Devices</i> .  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring AACL Rules on page 1058</a></li></ul>

## match-direction

---

<b>Syntax</b>	match-direction (input   output   input-output);
<b>Hierarchy Level</b>	[edit services aacl <a href="#">rule</a> rule-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the direction in which the rule match is applied.
<b>Options</b>	<p><b>input</b>—Apply the rule match on the input side of the interface.</p> <p><b>output</b>—Apply the rule match on the output side of the interface.</p> <p><b>input-output</b>—Apply the rule match bidirectionally.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Direction for ACL Rules on page 1059</a></li></ul>

## rule

<b>Syntax</b>	<pre> rule <i>rule-name</i> {   match-direction (input   output   input-output);   term <i>term-name</i> {     from {       application-group-any;       application-groups [ <i>application-group-names</i> ];       application-unknown;       applications [ <i>application-names</i> ];       destination-address <i>address</i> &lt;any-unicast&gt;;       destination-address-range low <i>minimum-value</i> high <i>maximum-value</i>;       destination-prefix-list <i>list-name</i>;       nested-application-unknown;       source-address <i>address</i> &lt;any-unicast&gt;;       source-address-range low <i>minimum-value</i> high <i>maximum-value</i>;       source-prefix-list <i>list-name</i>;     }     then {       (accept   discard);       count (application   application-group   application-group-any   nested-application           none);       forwarding-class <i>class-name</i>;       policer <i>policer-name</i>;     }   } } </pre>
<b>Hierarchy Level</b>	[edit services aacl], [edit services aacl <b>rule-set</b> <i>rule-set-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the rule the router uses when applying this service.
<b>Options</b>	<p><b>rule-name</b>—Identifier for the collection of terms that constitute this rule.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring AACL Rules on page 1058</a></li> </ul>

## rule-set (Services AACL)

---

<b>Syntax</b>	<code>rule-set <i>rule-set-name</i> {     [<i>rule</i> <i>rule-names</i>]; }</code>
<b>Hierarchy Level</b>	[edit services aacl]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<i>rule-set-name</i> —Identifier for the collection of rules that constitute this rule set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring AACL Rule Sets on page 1062</a></li></ul>

## services (AACL)

---

<b>Syntax</b>	<code>services aacl { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	<i>aacl</i> statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define the services to be applied to traffic.
<b>Options</b>	<i>aacl</i> —The values configured for application-aware-access-list matching rules.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Application-Aware Access List</i></li></ul>

## source-address (AACL)

---

<b>Syntax</b>	<code>source-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit services aacl <a href="#">rule rule-name</a> <a href="#">term term-name</a> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the source address for rule matching.
<b>Options</b>	<i>address</i> —Source IPv4 or IPv6 address or prefix value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in AACL Rules on page 1059</a></li></ul>

## source-address-range

---

<b>Syntax</b>	<code>source-address-range low <i>minimum-value</i> high <i>maximum-value</i>;</code>
<b>Hierarchy Level</b>	[edit services aacl <a href="#">rule rule-name</a> <a href="#">term term-name</a> <a href="#">from</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Specify the source address range for rule matching.
<b>Options</b>	<i>minimum-value</i> —Lower boundary for the IPv4 or IPv6 address range. <i>maximum-value</i> —Upper boundary for the IPv4 or IPv6 address range.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in AACL Rules on page 1059</a></li></ul>

## source-prefix-list

---

<b>Syntax</b>	<code>source-prefix-list <i>list-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services aacl <b>rule</b> <i>rule-name</i> <b>term</b> <i>term-name</i> <b>from</b>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the source prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the <code>[edit policy-options]</code> hierarchy level.
<b>Options</b>	<i>list-name</i> —Source prefix list.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Match Conditions in AACL Rules on page 1059</a></li></ul>

## term

**Syntax**    `term term-name {`  
                   `from {`  
                     `application-group-any;`  
                     `application-groups [ application-group-names ];`  
                     `application-unknown;`  
                     `applications [ application-names ];`  
                     `destination-address address <any-unicast>;`  
                     `destination-address-range low minimum-value high maximum-value;`  
                     `destination-prefix-list list-name;`  
                     `nested-application-unknown;`  
                     `source-address address <any-unicast>;`  
                     `source-address-range low minimum-value high maximum-value;`  
                     `source-prefix-list list-name;`  
                   `}`  
                   `then {`  
                     `(accept | discard);`  
                     `count (application | application-group | application-group-any | nested-application |`  
                       `none);`  
                     `forwarding-class class-name;`  
                     `policer policer-name;`  
                   `}`  
                   `}`

**Hierarchy Level**    [edit services aacl [rule](#) *rule-name*]

**Release Information**    Statement introduced in Junos OS Release 9.5.

**Description**    Define the AACL term properties.

**Options**    *term-name*—Identifier for the term.

The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                   interface-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring AACL Rules on page 1058](#)

## then

<b>Syntax</b>	<pre> then {   (accept   discard);   count (application   application-group   application-group-any   nested-application   none);   forwarding-class <i>class-name</i>;   log <i>event-type</i>;   policer <i>policer-name</i>; } </pre>
<b>Hierarchy Level</b>	[edit services aac <b>rule</b> <i>rule-name</i> <b>term</b> <i>term-name</i> ]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.5.</p> <p><b>policer</b> statement added in Junos OS Release 9.6.</p> <p>The <b>nested-application</b> option for the <b>count</b> statement introduced in Junos OS Release 11.1.</p>
<b>Description</b>	Define the ACL term actions. You can configure the router to accept or discard the targeted traffic. The action modifiers (count and forwarding-class) are optional.
<b>Options</b>	<p>You can configure one of the following actions:</p> <ul style="list-style-type: none"> <li>• <b>accept</b>—Accept the packets and all subsequent packets in flows that match the rules.</li> <li>• <b>discard</b>—Discard the packet and all subsequent packets in flows that match the rules.</li> </ul> <p>When you select <b>accept</b> as the action, you can optionally configure one or both of the following action modifiers. No action modifiers are allowed with the <b>discard</b> action.</p> <ul style="list-style-type: none"> <li>• <b>count (application   application-group   application-group-any   nested-application   none)</b>—For all accepted packets that match the rules, record a packet count using ACL statistics practices. You can specify one of the following options; there is no default setting: <ul style="list-style-type: none"> <li>• <b>application</b>—Count the application that matched in the <b>from</b> clause.</li> <li>• <b>application-group</b>—Count the application group that matched in the <b>from</b> clause.</li> <li>• <b>application-group-any</b>—Count all application groups that match <b>from application-group-any</b> under the <b>any</b> group name.</li> <li>• <b>nested-application</b>—Count all nested applications that matched in the <b>from</b> clause.</li> <li>• <b>none</b>—Same as not specifying <b>count</b> as an action.</li> </ul> </li> <li>• <b>forwarding-class <i>class-name</i></b>—Specify the packets' forwarding-class name.</li> </ul> <p><b>policer <i>policer-name</i></b>—Apply rate-limiting properties to the traffic as configured at the [edit firewall <b>policer</b> <i>policer-name</i>] hierarchy level. This configuration allows bit-rate and burst-size attributes to be applied to the traffic that are not supported by ACL rules. When you include a policer, the only allowed action is <b>discard</b>. For more information on policers, see the <i>Routing Policy Feature Guide for Routing Devices</i>.</p>

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring ACL Rules on page 1058</a></li><li>• <i>Routing Policy Feature Guide for Routing Devices</i></li></ul>

# Local Policy Decision Function Configuration Guidelines

Starting with Junos OS Release 12.1, the local policy decision function (L-PDF) plug-in can offload flows to the Packet Forwarding Engine. Offloading is supported only on MX Series routers with Modular Port Concentrators (MPCs) and accomplished using the Juniper Forwarding Mechanism (JFM). JFM allows services flows to be offloaded to the Packet Forwarding Engine. However, 5-tuple flows cannot be offloaded. Apart from the local L-PDF plug-in, offloading is supported on the packet-triggered subscribers and policy control (PTSP) plug-in. The **show services application-aware-access-list flows subscriber *subscriber-name*** command displays offload status.

This chapter includes the following sections:

- [Configuring Statistics Profiles on page 1079](#)
- [Applying L-PDF Profiles to Service Sets on page 1083](#)
- [Tracing L-PDF Operations on page 1084](#)

## Configuring Statistics Profiles

---

The local policy decision function (L-PDF) enables you to configure properties for statistics output. To do this, you create a statistics profile, which configures the files to which statistics records are exported and the format that is exported. There are two configurations you can use to specify the profile, as described in the following subsections:

- [Configuring an L-PDF Statistics Profile on page 1080](#)
- [Configuring an ACL Statistics Profile on page 1081](#)



**NOTE:** You must use the same configuration stanza for specifying the profile and the file selection. If configurations are committed in both hierarchies, the one at the `[edit system services local-policy-decision-function]` hierarchy level takes precedence.

---

**NOTE:**

- When a session closes before APPID has identified nested applications, the session is treated as a best-effort session and L-PDF does not get the nested application information. In such cases, nested applications will be reported as unknown applications.
- During the time that the application identification (APPID) feature has not yet made a final determination of the application associated with a given flow, the flow does not contribute to any per-subscriber or per-application statistics collection. For more information, see [“Best-Effort Application Identification of DPI-Serviced Flows” on page 988](#).



**NOTE:** For rms- interfaces, the statistics received from the active Multiservices PICs in the RMS group are combined with the statistics of the reported ended flows kept on the Routing Engine. The aggregated value is written to the statistics file. In the case of AMS interfaces, all the Multiservices PICs consisting of the AMS group reports statistics independently. These statistics are aggregated on the Routing Engine. The Routing Engine runs an independent timer, which on expiry writes the aggregated entry in the statistics file. This method of collection causes the statistics data in the statistics file to be displayed with a small delay.

## Configuring an L-PDF Statistics Profile

You can specify an L-PDF statistics profile by including the following configuration at the `[edit accounting-options]` hierarchy level:

```
[edit accounting-options]
policy-decision-statistics-profile profile-name {
  application-aware-access-list-fields [ field-name ];
  file filename;
  files number;
  size bytes;
}
```



**NOTE:** This configuration method is not the preferred method for configuring Junos Application Aware (previously known as Dynamic Application Awareness) statistics. It is only maintained for backwards compatibility and may be deprecated in a future software release and does not support the use of IPv6 address and prefix length. The new, preferred configuration is found at the `[edit system services local-policy-decision-function]` hierarchy level, as described in [“Configuring an ACL Statistics Profile” on page 1081](#). We encourage you to migrate to the new configuration method.

You specify a profile name to identify the profile and other properties as needed by including the `policy-decision-statistics-profile` statement. The `acl-fields` statement

specifies which statistics to collect in an accounting-data log file. This log file is located on the `/var/log` directory on the router. You specify the log file by including the **file filename** statement. The filename is prefixed by the **acl\_statistics\_** prefix; for example, if you specify the filename **lpdfd**, the log file will be `/var/log/acl_statistics_lpdfd`.

The **application-aware-access-list-fields** statement supports the following options:

- **address**—IP Address
- **application**—Application name
- **application-group**—Application group name
- **input-bytes**—Number of input bytes
- **input-interface**—Input interface name
- **input-packets**—Number of input packets
- **mask**—Netmask
- **output-bytes**—Number of output bytes
- **output-packets**—Number of output packets
- **subscriber-name**—Subscriber name
- **timestamp**—Timestamp
- **vrf-name**—VPN routing and forwarding (VRF) name

For more information on configuring profiles, see the *Network Management Administration Guide for Routing Devices*.

## Configuring an ACL Statistics Profile

You can specify an ACL statistics profile by including the following configuration at the **[edit system services]** hierarchy level:

```
local-policy-decision-function {
  statistics {
    file filename {
      archive-sites [ url ];
      files number;
      size bytes;
      transfer-interval minutes;
    }
    aacl-statistics-profile profile-name {
      aacl-fields [ field-name ];
      file filename;
      report-interval minutes;
      record-mode (interim-active-only | interim-full);
    }
    record-type (delta | interim);
  }
}
```

To specify the file properties, include the **file** statement at the **[edit system services local-policy-decision-function statistics]** hierarchy level with a unique filename:

- The **archive-sites** statement specifies one or more URLs for archiving the files. Archiving can be done by using FTP or SCP.
- The **files** statement specifies the maximum number of files that are maintained at one time.
- The **size** statement specifies the maximum size of each file.
- The **transfer-interval** statement specifies the interval between data transfers in minutes.

You specify a profile name to identify the profile and other properties as needed by including the **aacl-statistics-profile** statement. The **aacl-fields** statement specifies which statistics to collect in an accounting-data log file. This log file is located on the **/var/stats/aacl** directory on the router. You specify the log file by including the **file filename** statement.

The **aacl-fields** statement supports the following options:

- **address**—IP Address
- **all-fields**—All available fields
- **application**—Application name
- **application-group**—Application group name
- **input-bytes**—Number of input bytes
- **input-interface**—Input interface name
- **ipv6-address**—IPv6 address
- **ipv6-prefix-length**—Prefix length associated with the displayed IPv6 address
- **input-packets**—Number of input packets
- **mask**—Netmask
- **output-bytes**—Number of output bytes
- **output-packets**—Number of output packets
- **subscriber-name**—Subscriber name
- **timestamp**—Timestamp
- **vrf-name**—VPN routing and forwarding (VRF) name

The **record-type** statement specifies whether a record is **delta** or **interim**; **delta** is the default setting. The **report-interval** statement specifies the reporting interval in minutes; the default setting is 15 minutes and the range is 5 through 1440 minutes. The **record-mode** statement specifies how the statistics are reported for each reporting interval; the default setting is **interim-full** and reports all available statistics. To report only statistics that have changed for the reporting interval, use the **interim-active-only** setting.



**NOTE:** The IPv6 fields (`ipv6-address` and `ipv6-prefix-length`) are not supported for record-type delta. The IPv6 fields are supported for record-type interim only, meaning that the fields are restricted to the S- (Login) record.

For more information on configuring profiles, see the *Network Management Administration Guide for Routing Devices*.

#### Related Documentation

- [L-PDF Overview on page 986](#)
- [Best-Effort Application Identification of DPI-Serviced Flows on page 988](#)
- [Applying L-PDF Profiles to Service Sets on page 1083](#)
- [Tracing L-PDF Operations on page 1084](#)

## Applying L-PDF Profiles to Service Sets

You can optionally apply policy decision statistics profiles as part of a service-set definition. To do this, you include the **policy-decision-statistics-profile** statement at the **[edit services service-set service-set-name]** hierarchy level:

```
policy-decision-statistics-profile profile-name;
```



**NOTE:** To provide high availability for the policy decision statistics, associate the service-set definition with a redundant services PIC (rsp) interface.

You can include only one profile name in the specification for the **application-aware access-list** statement.

The following example shows a sample configuration for attachment of an L-PDF statistics profile:

```
services {
  service-set test_aacl_sset {
    aacl-rules aacl_rule;
    policy-decision-statistics-profile {
      pdf_stats_prof;
    }
    interface-service {
      service-interface ms-0/3/0.0;
    }
  }
}
```



**NOTE:** Only one service set can be applied to a single interface when L-PDF functionality is used.

The following example shows a sample configuration for attachment of a service set to a static interface:

```
interfaces {
  fe-0/0/0 {
    vlan-tagging;
    unit 1 {
      vlan-id 1;
      family inet {
        service {
          input {
            service-set test_aacl_sset;
          }
          output {
            service-set test_aacl_sset;
          }
        }
      }
      address 10.1.1.1/24;
    }
  }
}
```



**NOTE:** The `session-offload` statement at the `[edit chassis fpc slot-number pic number adaptive-services service-package extension-provider]` hierarchy level controls session offload behavior for Multiservices DPCs on MX Series routers. It controls session offload on a per-device basis, where a device is a Multiservices interface (`ms-fpc-pic-port`). Currently, the session offload function is supported for at most one Multiservices interface. When the offload function is enabled, it is strongly recommended that you limit Junos Application Aware (previously known as Dynamic Application Awareness) features to that Multiservices interface.

The default is to not offload any sessions. For more information on chassis configuration, see the *Junos OS Administration Library for Routing Devices*.

---

**Related  
Documentation**

- [L-PDF Overview on page 986](#)
- [Best-Effort Application Identification of DPI-Serviced Flows on page 988](#)
- [Configuring Statistics Profiles on page 1079](#)
- [Tracing L-PDF Operations on page 1084](#)

---

## Tracing L-PDF Operations

Tracing operations track L-PDF operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

By default, no events are traced. If you include the **traceoptions** statement at the **[edit system services local-policy-decision-function]** hierarchy level, you can customize the trace file settings:

```
traceoptions {  
  file filename <files number> <size size>;  
  flag flag;  
}
```

The flags track the following information:

- **all**—Everything
- **configuration**—Configuration traces
- **database**—Database traces
- **general**—Miscellaneous traces
- **gres**—Graceful Routing Engine switchover (GRES) traces
- **ptsp-statistics**—PTSP statistics traces
- **rtsock**—Routing socket traces
- **statistics**—Statistics traces
- **subscriber**—Subscriber traces

**Related  
Documentation**

- [L-PDF Overview on page 986](#)
- [Best-Effort Application Identification of DPI-Serviced Flows on page 988](#)
- [Configuring Statistics Profiles on page 1079](#)
- [Applying L-PDF Profiles to Service Sets on page 1083](#)



## CHAPTER 45

# Summary of L-PDF Configuration Statements

The following sections explain each of the local policy decision function (L-PDF) statements. The statements are organized alphabetically.

- [aacl-fields on page 1088](#)
- [aacl-statistics-profile on page 1089](#)
- [application-aware-access-list-fields on page 1090](#)
- [file on page 1091](#)
- [local-policy-decision-function on page 1092](#)
- [policy-decision-statistics-profile on page 1093](#)
- [statistics \(System Services\) on page 1094](#)
- [traceoptions \(Services Local Policy Decision Function\) on page 1095](#)

## aacl-fields

---

<b>Syntax</b>	<pre>aacl-fields {     <i>field-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit system services local-policy-decision-function statistics aacl-statistics-profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0. IPv6 support introduced in Junos OS Release 12.2
<b>Description</b>	Define the statistics to collect in a data log file.
<b>Options</b>	<p><i>field-name</i>—Name of the field:</p> <ul style="list-style-type: none"><li>• <b>address</b>—IPv4 address</li><li>• <b>all-fields</b>—All available fields</li><li>• <b>application</b>—Application name</li><li>• <b>application-group</b>—Application group name</li><li>• <b>input-bytes</b>—Number of input bytes</li><li>• <b>input-interface</b>—Input interface name</li><li>• <b>input-packets</b>—Number of input packets</li><li>• <b>ipv6-address</b>—IPv6 address</li><li>• <b>ipv6-prefix-length</b>—Prefix length associated with the displayed IPv6 address</li><li>• <b>mask</b>—Netmask</li><li>• <b>output-bytes</b>—Number of output bytes</li><li>• <b>output-packets</b>—Number of output packets</li><li>• <b>subscriber-name</b>—Subscriber name</li><li>• <b>timestamp</b>—Timestamp</li><li>• <b>vrf-name</b>—VPN routing and forwarding (VRF) name</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Statistics Profiles on page 1079</a></li></ul>

## aac1-statistics-profile

<b>Syntax</b>	<pre> aac1-statistics-profile <i>profile-name</i> {     aac1-fields {         <i>field-name</i>;     }     file <i>filename</i>;     record-mode (interim-active-only   interim-full);     report-interval <i>minutes</i>; } </pre>
<b>Hierarchy Level</b>	<pre> [edit services service-set <i>service-set-name</i>], [edit system services local-policy-decision-function statistics] </pre>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.0.</p> <p><b>record-mode</b> option introduced in Junos OS Release 10.2.</p>
<b>Description</b>	Create an AAC1 statistics profile, which configures the files to which statistics records are exported and the format that is exported.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the statistics data output. Enclose the name within quotation marks. All files are placed in the directory <code>/var/stats/aac1</code>.</p> <p><b>record-mode</b>—Record mode for the reporting interval; possible values are <b>interim-active-only</b>, which reports only statistics that have changed, or <b>interim-full</b>, which reports all available statistics.</p> <p><b>report-interval <i>minutes</i></b>—Frequency at which statistics are recorded, in minutes.</p> <p><b>Default:</b> 15 minutes</p> <p><b>Range:</b> 5 through 1440 minutes</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>For more information on profiles, see the <i>Network Management Administration Guide for Routing Devices</i>.</li> <li><a href="#">Configuring Statistics Profiles on page 1079</a></li> </ul>

## application-aware-access-list-fields

---

<b>Syntax</b>	<pre>application-aware-access-list-fields {     <i>field-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit accounting-options policy-decision-statistics-profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Define the statistics to collect in a data log file.
<b>Options</b>	<p><i>field-name</i>—Name of the field:</p> <ul style="list-style-type: none"><li>• <b>address</b>—IP address</li><li>• <b>application</b>—Application name</li><li>• <b>application-group</b>—Application group name</li><li>• <b>input-bytes</b>—Number of input bytes</li><li>• <b>input-interface</b>—Input interface name</li><li>• <b>input-packets</b>—Number of input packets</li><li>• <b>mask</b>—Netmask</li><li>• <b>output-bytes</b>—Number of output bytes</li><li>• <b>output-packets</b>—Number of output packets</li><li>• <b>subscriber-name</b>—Subscriber name</li><li>• <b>timestamp</b>—Timestamp</li><li>• <b>vrf-name</b>—VPN routing and forwarding (VRF) name</li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Statistics Profiles on page 1079</a></li></ul>

## file

---

<b>Syntax</b>	<pre>file <i>file-name</i> {     archive-sites <i>url</i>;     files <i>file-number</i>;     size <i>bytes</i>;     transfer-interval <i>minutes</i>; }</pre>
<b>Hierarchy Level</b>	[edit system services local-policy-decision-function statistics]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a file to which statistics records are exported and the format that is exported.
<b>Options</b>	<p><b>archive-sites</b> [<i>url</i>]<b>—</b>One or more destinations for archiving data.</p> <p><b>filename</b><b>—</b>Name of the file to receive the statistics data output.</p> <p><b>files</b> <i>number</i><b>—</b>(Optional) Maximum number of accounting files.  <b>Range:</b> 3 through 1000 files  <b>Default:</b> 3 files</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>size</b> <i>size</i><b>—</b>(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  <b>Syntax:</b> <i>xk</i> to specify KB, <i>xm</i> to specify MB, or <i>xg</i> to specify GB  <b>Range:</b> 262144 through 1073741824 or the maximum file size supported on your system</p> <p>If you specify a maximum file size, you also must specify a maximum number of trace files with the <b>files</b> option.</p> <p><b>transfer-interval</b> <i>minutes</i><b>—</b>Frequency at which to transfer files to archive sites, in minutes.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Statistics Profiles on page 1079</a></li> </ul>

## local-policy-decision-function

---

**Syntax**    local-policy-decision-function {  
              statistics {  
                  aocl-statistics-profile *profile-name* {  
                      aocl-fields {  
                          *field-name*;  
                      }  
                      file *filename*;  
                      report-interval *minutes*;  
                  }  
                  file *file-name* {  
                      archive-sites *url*;  
                      files *file-number*;  
                      size *bytes*;  
                      transfer-interval *minutes*;  
                  }  
                  record-type (delta | interim);  
              }  
              traceoptions {  
                  file *filename* <files *number*> <size *size*>;  
                  flag *flag*;  
                  no-remote-trace;  
              }  
          }

**Hierarchy Level**    [edit system services]

**Release Information**    Statement introduced in Junos OS Release 10.0.

**Description**    Specify L-PDF properties.

**Options**    The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring Statistics Profiles on page 1079](#)

## policy-decision-statistics-profile

<b>Syntax</b>	<pre> policy-decision-statistics-profile <i>profile-name</i> {     aacl-fields {         <i>field-name</i>;     }     file <i>filename</i>;     files <i>file-number</i>;     size <i>bytes</i>; } </pre>
<b>Hierarchy Level</b>	[edit accounting-options], [edit services service-set <i>service-set-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Create a policy decision statistics profile, which configures the files to which statistics records are exported and the format that is exported.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the accounting-data output. Enclose the name within quotation marks. All files are placed in the directory <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of accounting files.  <b>Range:</b> 2 through 1000 files  <b>Default:</b> 2 files</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b><i>profile-name</i></b>—Name of the policy decision statistics profile.</p> <p><b>size <i>size</i></b>—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).  <b>Syntax:</b> <b>xk</b> to specify KB, <b>xm</b> to specify MB, or <b>xg</b> to specify GB  <b>Range:</b> 10240 through 1073741824 or the maximum file size supported on your system</p> <p>If you specify a maximum file size, you also must specify a maximum number of trace files with the <b>files</b> option.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>For more information on profiles, see the <i>Network Management Administration Guide for Routing Devices</i>.</li> <li><a href="#">Configuring Statistics Profiles on page 1079</a></li> </ul>

## statistics (System Services)

---

**Syntax**

```
statistics {  
  aacl-statistics-profile profile-name {  
    aacl-fields {  
      field-name;  
    }  
    file filename;  
    report-interval minutes;  
  }  
  file file-name {  
    archive-sites [ url ];  
    files file-number;  
    size bytes;  
    transfer-interval minutes;  
  }  
  record-type (delta | interim);  
}
```

**Hierarchy Level** [edit system services local-policy-decision-function]

**Release Information** Statement introduced in Junos OS Release 10.0.

**Description** Configure file and data specifications for recording AACL statistics.

**Options** **record-type**—Record type; possible values are **delta** or **interim**.

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Statistics Profiles on page 1079](#)

## traceoptions (Services Local Policy Decision Function)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt;;     flag <i>flag</i>;     no-remote-trace; } </pre>
<b>Hierarchy Level</b>	[edit services local-policy-decision-function], [edit system services local-policy-decision-function]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure local policy decision function (L-PDF) tracing options.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b><i>trace-file</i></b> reaches its maximum size, it is renamed <b><i>trace-file.0</i></b>, then <b><i>trace-file.1</i></b>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p><b>Range:</b> 2 through 1000 files</p> <p><b>Default:</b> 2 files</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b><i>flag</i></b>—Tracing operation to perform. To specify more than one flag, include multiple <b>flag</b> statements.</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Everything</li> <li>• <b>configuration</b>—Configuration traces</li> <li>• <b>database</b>—Database traces</li> <li>• <b>general</b>—Miscellaneous traces</li> <li>• <b>gres</b>—Graceful Routing Engine switchover (GRES) traces</li> <li>• <b>ptsp-statistics</b>—PTSP statistics traces</li> <li>• <b>rtsock</b>—Routing socket traces</li> <li>• <b>statistics</b>—Statistics traces</li> <li>• <b>subscriber</b>—Subscriber traces</li> </ul> <p><b>no-remote-trace</b>—Disable remote tracing.</p> <p><b>size <i>size</i></b>—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named <b><i>trace-file</i></b> reaches this size, it is renamed <b><i>trace-file.0</i></b>. When the <b><i>trace-file</i></b> again reaches its maximum size, <b><i>trace-file.0</i></b> is renamed</p>

*trace-file.1* and *trace-file* is renamed *trace-file.0*. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

**Syntax:** *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB

**Range:** 10240 through 1073741824 or the maximum file size supported on your system

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

<b>Required Privilege</b>	routing and trace—To view this statement in the configuration.
<b>Level</b>	routing-control and trace-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Tracing L-PDF Operations on page 1084</a></li></ul>

## PART 4

# Encryption Services

- [Encryption Overview on page 1099](#)
- [Encryption Interfaces Configuration Guidelines on page 1101](#)
- [Summary of Encryption Configuration Statements on page 1111](#)



# Encryption Overview

This chapter discusses the following topics:

- [Encryption Overview on page 1099](#)

## Encryption Overview

---

The IP Security (IPsec) architecture provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. It also defines mechanisms for key generation and exchange, management of security associations, and support for digital certificates.

IPsec defines a security association (SA) and key management framework that can be used with any network layer protocol. The SA specifies what protection policy to apply to traffic between two IP-layer entities. For more information, see the *Junos OS Administration Library for Routing Devices*. The standards are defined in the following RFCs:

- RFC 2401, *Security Architecture for the Internet Protocol*
- RFC 2406, *IP Encapsulating Security Payload (ESP)*

### Related Documentation

- [Configuring Encryption Interfaces on page 1101](#)
- [Configuring Filters for Traffic Transiting the ES PIC on page 1103](#)
- [Configuring ES PIC Redundancy on page 1109](#)
- [Configuring IPsec Tunnel Redundancy on page 1110](#)



# Encryption Interfaces Configuration Guidelines

To enable encryption interfaces, you can configure the following properties:

- [Configuring Encryption Interfaces on page 1101](#)
- [Configuring Filters for Traffic Transiting the ES PIC on page 1103](#)
- [Configuring an ES Tunnel Interface for a Layer 3 VPN on page 1108](#)
- [Configuring ES PIC Redundancy on page 1109](#)
- [Configuring IPsec Tunnel Redundancy on page 1110](#)

## Configuring Encryption Interfaces

---

When you configure the encryption interface, you associate the configured SA with a logical interface. This configuration defines the tunnel, including the logical unit, tunnel addresses, maximum transmission unit (MTU), optional interface addresses, and the name of the IPsec SA to apply to traffic. To configure an encryption interface, include the following statements at the `[edit interfaces es-fpc/pic/port unit logical-unit-number]` hierarchy level:

```
family inet {  
  ipsec-sa ipsec-sa; # name of security association to apply to packet  
  address address; # local interface address inside local VPN  
  destination address; # destination address inside remote VPN  
}  
tunnel {  
  source source-address;  
  destination destination-address;  
}
```

The addresses configured as the tunnel source and destination are the addresses in the outer IP header of the tunnel.



**NOTE:** You must configure the tunnel source address locally on the router, and the tunnel destination address must be a valid address for the security gateway terminating the tunnel.

The ES Physical Interface Card (PIC) is supported on M Series and T Series routers.

The SA must be a valid tunnel-mode SA. The interface address and destination address listed are optional. The destination address allows the user to configure a static route to encrypt traffic. If a static route uses that destination address as the next hop, traffic is forwarded through the portion of the tunnel in which encryption occurs.

## Specifying the Security Association Name for Encryption Interfaces

The security association is the set of properties that defines the protocols for encrypting Internet traffic. To configure encryption interfaces, you specify the SA name associated with the interface by including the `ipsec-sa` statement at the `[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]` hierarchy level:

```
ipsec-sa sa-name;
```

For information about configuring the security association, see “Configuring Filters for Traffic Transiting the ES PIC” on page 1103.

## Configuring the MTU for Encryption Interfaces

The protocol MTU value for encryption interfaces must always be less than the default interface MTU value of 3900 bytes; the configuration fails to commit if you select a greater value. To set the MTU value, include the `mtu` statement at the `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy level:

```
mtu bytes;
```

For more information, see the *Junos OS Network Interfaces Library for Routing Devices*.

## Example: Configuring an Encryption Interface

Configure an IPsec tunnel as a logical interface on the ES PIC. The logical interface specifies the tunnel through which the encrypted traffic travels. The `ipsec-sa` statement associates the security profile with the interface.

```
[edit interfaces]
es-0/0/0 {
  unit 0 {
    tunnel {
      source 10.5.5.5; # tunnel source address
      destination 10.6.6.6; # tunnel destination address
    }
    family inet {
      ipsec-sa manual-sa1; # name of security association to apply to packet
      mtu 3800;
      address 10.1.1.8/32 { # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
    }
  }
}
```

```

    }
  }
}

```

#### Related Documentation

- [Encryption Overview on page 1099](#)
- [Configuring Filters for Traffic Transiting the ES PIC on page 1103](#)
- [Configuring ES PIC Redundancy on page 1109](#)
- [Configuring IPsec Tunnel Redundancy on page 1110](#)

## Configuring Filters for Traffic Transiting the ES PIC

This section contains the following topics:

- [Traffic Overview on page 1103](#)
- [Configuring the Security Association on page 1104](#)
- [Configuring an Outbound Traffic Filter on page 1105](#)
- [Applying the Outbound Traffic Filter on page 1106](#)
- [Configuring an Inbound Traffic Filter on page 1106](#)
- [Applying the Inbound Traffic Filter to the Encryption Interface on page 1107](#)

### Traffic Overview

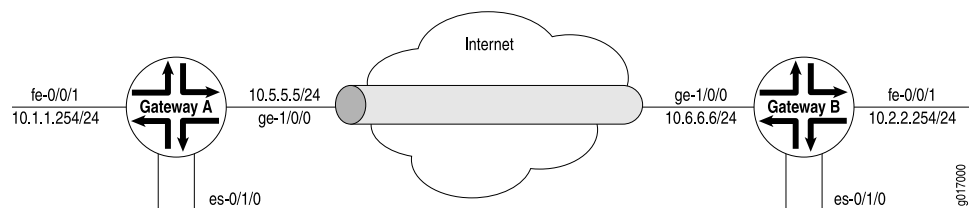
Traffic configuration defines the traffic that must flow through the tunnel. You configure outbound and inbound firewall filters, which identify and direct traffic to be encrypted and confirm that decrypted traffic parameters match those defined for the given tunnel. The outbound filter is applied to the LAN or WAN interface for the incoming traffic you want to encrypt. The inbound filter is applied to the ES PIC to check the policy for traffic coming in from the remote host. Because of the complexity of configuring a router to forward packets, no automatic checking is done to ensure that the configuration is correct.



**NOTE:** The valid firewall filters statements for IPsec are **destination-port**, **source-port**, **protocol**, **destination-address**, and **source-address**.

In [Figure 18 on page 1103](#), Gateway A protects the network 10.1.1.0/24, and Gateway B protects the network 10.2.2.0/24. The gateways are connected by an IPsec tunnel. For more information about firewalls, see the *Routing Policy Feature Guide for Routing Devices*.

**Figure 18: Example: IPsec Tunnel Connecting Security Gateways**



The SA and ES interface for security Gateway A are configured as follows:

```
[edit security ipsec]
security-association manual-sa1 {
  manual {
    direction bidirectional {
      protocol esp;
      spi 2312;
      authentication {
        algorithm hmac-md5-96;
        key ascii-text 1234123412341234;
      }
      encryption {
        algorithm 3des-cbc;
        key ascii-text 123456789009876543211234;
      }
    }
  }
}
[edit interfaces es-0/1/0]
unit 0 {
  tunnel {
    source 10.5.5.5;
    destination 10.6.6.6;
  }
  family inet {
    ipsec-sa manual-sa1;
    address 10.1.1.8/32 {
      destination 10.2.2.254;
    }
  }
}
```

## Configuring the Security Association

To configure the SA, include the **security-association** statement at the **[edit security]** hierarchy level:

```
security-association name {
  mode (tunnel | transport);
  manual {
    direction (inbound | outbound | bi-directional) {
      auxiliary-spi auxiliary-spi-value;
      spi spi-value;
      protocol (ah | esp | bundle);
      authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
      }
    }
  }
  dynamic {
    replay-window-size (32 | 64);
  }
}
```

```

        ipsec-policy policy-name;
    }
}

```

For more information about configuring an SA, see the *Junos OS Administration Library for Routing Devices*. For information about applying the SA to an interface, see [“Specifying the Security Association Name for Encryption Interfaces” on page 1102](#).

## Configuring an Outbound Traffic Filter

To configure the outbound traffic filter, include the **filter** statement at the **[edit firewall]** hierarchy level:

```

filter filter-name {
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
      action-modifiers;
    }
  }
}

```

For more information, see the *Routing Policy Feature Guide for Routing Devices*.

### Example: Configuring an Outbound Traffic Filter

Firewall filters for outbound traffic direct the traffic through the desired IPsec tunnel and ensure that the tunneled traffic goes out the appropriate interface (see [Figure 18 on page 1103](#)). Here, an outbound firewall filter is created on security Gateway A; it identifies the traffic to be encrypted and adds it to the input side of the interface that carries the internal virtual private network (VPN) traffic:

```

[edit firewall]
filter ipsec-encrypt-policy-filter {
  term term1 {
    from {
      source-address { # local network
        10.1.1.0/24;
      }
      destination-address { # remote network
        10.2.2.0/24;
      }
    }
  }
  then ipsec-sa manual-sa1; # apply SA name to packet
  term default {
    then accept;
  }
}

```



**NOTE:** The source address, port, and protocol on the outbound traffic filter must match the destination address, port, and protocol on the inbound traffic filter. The destination address, port, and protocol on the outbound traffic filter must match the source address, port, and protocol on the inbound traffic filter.

## Applying the Outbound Traffic Filter

After you have configured the outbound firewall filter, you apply it by including the **filter** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet]** hierarchy level:

```
filter {
  input filter-name;
}
```

### Example: Applying the Outbound Traffic Filter

Apply the outbound traffic filter. The outbound filter is applied on the Fast Ethernet interface at the **[edit interfaces *fe-0/0/1* unit 0 family inet]** hierarchy level. Any packet matching the IPsec action term (**term 1**) on the input filter (**ipsec-encrypt-policy-filter**), configured on the Fast Ethernet interface, is directed to the ES PIC interface at the **[edit interfaces *es-0/1/0* unit 0 family inet]** hierarchy level. So, if a packet arrives from the source address **10.1.1.0/24** and goes to the destination address **10.2.2.0/24**, the Packet Forwarding Engine directs the packet to the ES PIC interface, which is configured with the **manual-sa1** SA. The ES PIC receives the packet, applies the **manual-sa1** SA, and sends the packet through the tunnel.

The router must have a route to the tunnel end point; add a static route if necessary.

```
[edit interfaces]
fe-0/0/1 {
  unit 0 {
    family inet {
      filter {
        input ipsec-encrypt-policy-filter;
      }
      address 10.1.1.254/24;
    }
  }
}
```

## Configuring an Inbound Traffic Filter

To configure an inbound traffic filter, include the **filter** statement at the **[edit firewall]** hierarchy level:

```
filter filter-name {
  term term-name {
    from {
      match-conditions;
    }
  }
}
```

```

    then {
        action;
        action-modifiers;
    }
}

```

For more information, see the *Routing Policy Feature Guide for Routing Devices*.

### Example: Configuring an Inbound Traffic Filter

Configure an inbound firewall filter. This filter performs the final IPsec policy check and is created on security gateway A. The policy check ensures that only packets that match the traffic configured for this tunnel are accepted.

```

[edit firewall]
filter ipsec-decrypt-policy-filter {
  term term1 { # perform policy check
    from {
      source-address { # remote network
        10.2.2.0/24;
      }
      destination-address { # local network
        10.1.1.0/24;
      }
    }
  }
}
then accept;

```

### Applying the Inbound Traffic Filter to the Encryption Interface

After you create the inbound firewall filter, you can apply it to the ES PIC. To apply the filter to the ES PIC, include the **filter** statement at the **[edit interfaces es-fpc/pic/port unit logical-unit-number family inet filter]** hierarchy level:

```

filter {
  input filter;
}

```

The input filter is the name of the filter applied to received traffic. For a configuration example, see “[Example: Configuring an Inbound Traffic Filter](#)” on page 1107. For more information about firewall filters, see the *Routing Policy Feature Guide for Routing Devices*.

### Example: Applying the Inbound Traffic Filter to the Encryption Interface

Apply the inbound firewall filter (**ipsec-decrypt-policy-filter**) to the decrypted packet to perform the final policy check. The IPsec **manual-sa1** SA is referenced at the **[edit interfaces es-1/2/0 unit 0 family inet]** hierarchy level and decrypts the incoming packet.

The Packet Forwarding Engine directs IPsec packets to the ES PIC. It uses the packet's security parameter index (SPI), protocol, and destination address to look up the SA configured on one of the ES interfaces. The IPsec **manual-sa1** SA is referenced at the **[edit interfaces es-1/2/0 unit 0 family inet]** hierarchy level and is used to decrypt the incoming packet. When the packets are processed (decrypted, authenticated, or both), the input firewall filter (**ipsec-decrypt-policy-filter**) is applied on the decrypted packet to perform the final policy check. **term1** defines the decrypted (and verified) traffic and

performs the required policy check. For information about **term1**, see [“Example: Configuring an Inbound Traffic Filter” on page 1107](#).



**NOTE:** The inbound traffic filter is applied after the ES PIC has processed the packet, so the decrypted traffic is defined as any traffic that the remote gateway is encrypting and sending to this router. IKE uses this filter to determine the policy required for a tunnel. This policy is used during the negotiation with the remote gateway to find the matching SA configuration.

```
[edit interfaces]
es-1/2/0 {
  unit 0 {
    tunnel {
      source 10.5.5.5; # tunnel source address
      destination 10.6.6.6; # tunnel destination address
    }
    family inet {
      filter {
        input ipsec-decrypt-policy-filter;
      }
      ipsec-sa manual-sa1; # SA name applied to packet
      address 10.1.1.8/32 { # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
    }
  }
}
```

**Related  
Documentation**

- [Encryption Overview on page 1099](#)
- [Configuring Encryption Interfaces on page 1101](#)
- [Configuring ES PIC Redundancy on page 1109](#)
- [Configuring IPsec Tunnel Redundancy on page 1110](#)

---

## Configuring an ES Tunnel Interface for a Layer 3 VPN

---

To configure an ES tunnel interface for a Layer 3 VPN, you need to configure an ES tunnel interface on the provider edge (PE) router and on the customer edge (CE) router. You also need to configure IPsec on the PE and CE routers. For more information about configuring an ES tunnel for a Layer 3 VPN, see the *Junos OS VPNs Library for Routing Devices*.

**Related  
Documentation**

- [Encryption Overview on page 1099](#)
- [Configuring Encryption Interfaces on page 1101](#)
- [Configuring Filters for Traffic Transiting the ES PIC on page 1103](#)
- [Configuring ES PIC Redundancy on page 1109](#)
- [Configuring IPsec Tunnel Redundancy on page 1110](#)

## Configuring ES PIC Redundancy

You can configure ES PIC redundancy on M Series and T Series routers that have multiple ES PICs. With ES PIC redundancy, one ES PIC is active and another ES PIC is on standby. When the primary ES PIC has a servicing failure, the backup becomes active, inherits all the tunnels and SAs, and acts as the new next hop for IPsec traffic. Reestablishment of tunnels on the backup ES PIC does not require new Internet Key Exchange (IKE) negotiations. If the primary ES PIC comes online, it remains in standby and does not preempt the backup. To determine which PIC is currently active, use the **show ipsec redundancy** command.



**NOTE:** ES PIC redundancy is supported on M Series and T Series routers.

To configure an ES PIC as the backup, include the **backup-interface** statement at the **[edit interfaces fpc/pic/port es-options]** hierarchy level:

```
backup-interface es-fpc/pic/port;
```

### Example: Configuring ES PIC Redundancy

After you create the inbound firewall filter, apply it to the master ES PIC. Here, the inbound firewall filter (**ipsec-decrypt-policy-filter**) is applied on the decrypted packet to perform the final policy check. The IPsec **manual-sa1** SA is referenced at the **[edit interfaces es-1/2/0 unit 0 family inet]** hierarchy level and decrypts the incoming packet. This example does not show SA and filter configuration. For information about SA and filter configuration, see the *Junos OS Administration Library for Routing Devices*, the *Routing Policy Feature Guide for Routing Devices*, and [“Example: Configuring an Inbound Traffic Filter” on page 1107](#).

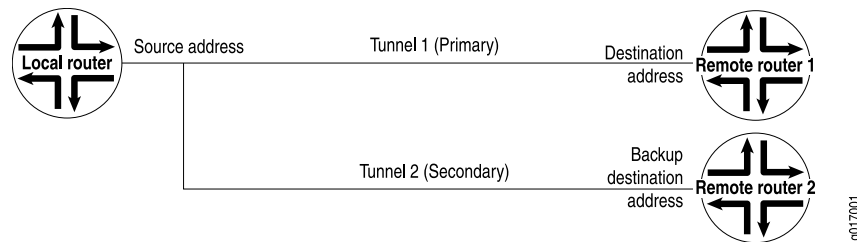
```
[edit interfaces]
es-1/2/0 {
  es-options {
    backup-interface es-1/0/0;
  }
  unit 0 {
    tunnel {
      source 10.5.5.5;
      destination 10.6.6.6;
    }
    family inet {
      ipsec-sa manual-sa1;
      filter {
        input ipsec-decrypt-policy-filter;
      }
      address 10.1.1.8/32 {
        destination 10.2.2.254;
      }
    }
  }
}
```

- Related Documentation**
- [Encryption Overview on page 1099](#)
  - [Configuring Encryption Interfaces on page 1101](#)
  - [Configuring Filters for Traffic Transiting the ES PIC on page 1103](#)
  - [Configuring IPsec Tunnel Redundancy on page 1110](#)

## Configuring IPsec Tunnel Redundancy

You can configure IPsec tunnel redundancy by specifying a backup destination address. The local router sends keepalives to determine the remote site's reachability. When the peer is no longer reachable, a new tunnel is established. For up to 60 seconds during failover, traffic is dropped without notification being sent. [Figure 19 on page 1110](#) shows IPsec primary and backup tunnels.

**Figure 19: IPsec Tunnel Redundancy**



To configure IPsec tunnel redundancy, include the **backup-destination** statement at the [edit interfaces unit *logical-unit-number* tunnel] hierarchy level:

```

backup-destination address;
destination address;
source address;

```



**NOTE:** Tunnel redundancy is supported on M Series and T Series routers.

The primary and backup destinations must be on different routers.

The tunnels must be distinct from each other and policies must match.

For more information about tunnels, see *Tunnel Properties*.

- Related Documentation**
- [Encryption Overview on page 1099](#)
  - [Configuring Encryption Interfaces on page 1101](#)
  - [Configuring Filters for Traffic Transiting the ES PIC on page 1103](#)
  - [Configuring ES PIC Redundancy on page 1109](#)

## CHAPTER 48

# Summary of Encryption Configuration Statements

The following sections explain each of the encryption services statements. The statements are organized alphabetically.

### address (Interfaces)

---

<b>Syntax</b>	<code>address <i>address</i> {     <i>destination address</i>; }</code>
<b>Hierarchy Level</b>	[edit <code>interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i></code> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the interface address.
<b>Options</b>	<code><i>address</i></code> —Address of the interface.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Encryption Interfaces on page 1101</a></li></ul>

### backup-destination

---

See [backup-destination](#)

## backup-interface

---

<b>Syntax</b>	<code>backup-interface <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit interfaces <i>interface-name</i> <a href="#">es-options</a>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure a backup ES Physical Interface Card (PIC). When the primary ES PIC has a servicing failure, the backup becomes active, inherits all the tunnels and security associations (SAs), and acts as the new next hop for IPsec traffic.
<b>Options</b>	<i>interface-name</i> —Name of ES interface to serve as the backup.
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring ES PIC Redundancy on page 1109</a></li></ul>

## destination (Interfaces)

<b>Syntax</b>	<code>destination address;</code>
<b>Hierarchy Level</b>	<p>[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> tunnel]</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet address <i>address</i>],</p> <p>[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> tunnel]</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet address <i>address</i>]</p>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For CoS on ATM interfaces, specify the remote address of the connection.</p> <p>For point-to-point interfaces only, specify the address of the interface at the remote end of the connection.</p> <p>For tunnel and encryption interfaces, specify the remote address of the tunnel.</p>
<b>Options</b>	<b>address</b> —Address of the remote side of the connection.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Linear RED Profiles on ATM Interfaces</a></li> <li>• <a href="#">Multilink and Link Services Logical Interface Configuration Overview on page 1385</a></li> <li>• <a href="#">Configuring Encryption Interfaces on page 1101</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> <li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li> <li>• <a href="#">Configuring Unicast Tunnels on page 1567</a></li> </ul>

## es-options

---

<b>Syntax</b>	<pre>es-options {   backup-interface <i>interface-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>On ES interfaces, configure ES interface-specific interface properties.</p> <p>The <b>backup-interface</b> statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring ES PIC Redundancy on page 1109</a></li></ul>

## family

<b>Syntax</b>	family inet { ipsec-sa sa-name; }
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure protocol family information for the logical interface.
<b>Options</b>	<p><b>family</b>—Protocol family:</p> <ul style="list-style-type: none"> <li>• <b>ccc</b>—Circuit cross-connect protocol suite</li> <li>• <b>inet</b>—IP version 4 suite</li> <li>• <b>inet6</b>—IP version 6 suite</li> <li>• <b>iso</b>—Open Systems Interconnection (OSI) International Organization for Standardization (ISO) protocol suite</li> <li>• <b>mlfr-end-to-end</b>—Multilink Frame Relay FRF.15</li> <li>• <b>mlfr-uni-nni</b>—Multilink Frame Relay FRF.16</li> <li>• <b>multilink-ppp</b>—Multilink Point-to-Point Protocol</li> <li>• <b>mpls</b>—MPLS</li> <li>• <b>tcc</b>—Translational cross-connect protocol suite</li> <li>• <b>tnp</b>—Trivial Network Protocol</li> <li>• <b>vpls</b>—Virtual private LAN service</li> </ul> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Encryption Interfaces on page 1101</a></li> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li> </ul>

## filter

---

<b>Syntax</b>	<pre>filter {     input <i>filter-name</i>;     output <i>filter-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> unit <i>logical-unit-number</i> family inet]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the filters to be applied on an interface.
<b>Options</b>	<p><b>input <i>filter-name</i></b>—Identifier for the input filter.</p> <p><b>output <i>filter-name</i></b>—Identifier for the output filter.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Filters for Traffic Transiting the ES PIC on page 1103</a></li></ul>

## interfaces

---

<b>Syntax</b>	<pre>interfaces { ... }</pre>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure interfaces on the router.
<b>Default</b>	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Junos OS Network Interfaces Library for Routing Devices</a></li></ul>

## ipsec-sa

---

<b>Syntax</b>	<code>ipsec-sa sa-name;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>es-fpc/pic/port</i> <b>unit</b> <i>logical-unit-number</i> family inet]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the IP Security (IPsec) SA name associated with the interface.
<b>Options</b>	<b>sa-name</b> —IPsec SA name.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Encryption Interfaces on page 1101</a></li> <li>• <i>Junos OS Administration Library for Routing Devices</i></li> </ul>

## source

---

<b>Syntax</b>	<code>source source-address;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet <b>address</b> <i>address</i> ], [edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> tunnel]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For tunnel and encryption interfaces, specify the source address.
<b>Options</b>	<b>source-address</b> —Address of the source side of the connection.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Encryption Interfaces on page 1101</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> <li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li> </ul>

## tunnel

---

**Syntax**    tunnel {  
              `backup-destination` *destination-address*;  
              `destination` *destination-address*;  
              `routing-instance` {  
                  `destination` *routing-instance-name*;  
              }  
              `source` *source-address*;  
              `ttl` *number*;  
          }

**Hierarchy Level**    [edit interfaces *interface-name* `unit` *logical-unit-number*]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure a tunnel. You can use the tunnel for unicast and multicast traffic or just for multicast traffic. You can also use tunnels for encrypted traffic or virtual private networks (VPNs).

The statements are explained separately.

**Required Privilege**    interface—To view this statement in the configuration.  
**Level**    interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Encryption Interfaces on page 1101](#)
- *Tunnel Properties*
- *Junos OS VPNs Library for Routing Devices*

## unit (Interfaces)

<b>Syntax</b>	<pre> unit <i>logical-unit-number</i> {     family inet {         ipsec-sa <i>sa-name</i>;     }     tunnel {         backup-destination <i>destination-address</i>;         destination <i>destination-address</i>;         routing-instance {             destination <i>routing-instance-name</i>;         }         source <i>source-address</i>;         ttl <i>number</i>;     } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
<b>Options</b>	<p><b><i>logical-unit-number</i></b>—Number of the logical unit.</p> <p><b>Range:</b> 0 through 16,384</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Encryption Interfaces on page 1101</a></li> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li> </ul>



## PART 5

# Flow Monitoring and Discard Accounting Services

- [Flow Monitoring and Discard Accounting Overview on page 1123](#)
- [Flow Monitoring and Discard Accounting Configuration Guidelines on page 1129](#)
- [Summary of Flow-Monitoring Configuration Statements on page 1213](#)
- [Flow Collection Configuration Guidelines on page 1295](#)
- [Summary of Flow Collection Configuration Statements on page 1309](#)
- [Dynamic Flow Capture Configuration Guidelines on page 1327](#)
- [Flow-Tap Configuration Guidelines on page 1339](#)
- [Summary of Dynamic Flow Capture and Flow-Tap Configuration Statements on page 1349](#)



# Flow Monitoring and Discard Accounting Overview

Using a Juniper Networks M Series Multiservice Edge or T Series Core Router, a selection of PICs (including the Monitoring Services PIC, Adaptive Services [AS] PIC, Multiservices PIC, or Multiservices DPC) and other networking hardware, you can monitor traffic flow and export the monitored traffic. Monitoring traffic allows you to do the following:

- Gather and export detailed information about IP version 4 (IPv4) traffic flows between source and destination nodes in your network.
- Sample all incoming IPv4 traffic on the monitoring interface and present the data in cflowd record format.
- Perform discard accounting on an incoming traffic flow.
- Encrypt or tunnel outgoing cflowd records, intercepted IPv4 traffic, or both.
- Direct filtered traffic to different packet analyzers and present the data in its original format (port mirror).



**NOTE:** Monitoring Services PICs, AS PICs, and Multiservices PICs must be mounted on an Enhanced Flexible PIC Concentrator (FPC) in an M Series or T Series router.

Multiservices DPCs installed in Juniper Networks MX Series 3D Universal Edge Routers support the same functionality, with the exception of the passive monitoring and flow-tap features.

This section provides general information on the following topics:

- [Passive Flow Monitoring Overview on page 1124](#)
- [Active Flow Monitoring Overview on page 1125](#)

## Passive Flow Monitoring Overview

Using a Juniper Networks M Series Multiservice Edge or T Series Core Router, a selection of PICs (including the Monitoring Services PIC, Adaptive Services [AS] PIC, Multiservices PIC, or Multiservices DPC) and other networking hardware, you can monitor traffic flow and export the monitored traffic. Monitoring traffic allows you to do the following:

- Gather and export detailed information about IP version 4 (IPv4) traffic flows between source and destination nodes in your network.
- Sample all incoming IPv4 traffic on the monitoring interface and present the data in cflowd record format.
- Perform discard accounting on an incoming traffic flow.
- Encrypt or tunnel outgoing cflowd records, intercepted IPv4 traffic, or both.
- Direct filtered traffic to different packet analyzers and present the data in its original format (port mirror).

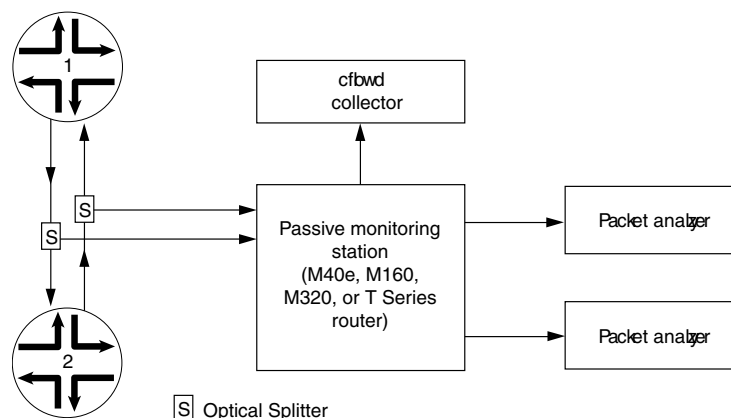


**NOTE:** Monitoring Services PICs, AS PICs, and Multiservices PICs must be mounted on an Enhanced Flexible PIC Concentrator (FPC) in an M Series or T Series router.

Multiservices DPCs installed in Juniper Networks MX Series 3D Universal Edge Routers support the same functionality, with the exception of the passive monitoring and flow-tap features.

The router used for passive monitoring does not route packets from the monitored interface, nor does it run any routing protocols related to those interfaces; it only receives traffic flows, collects intercepted traffic, and exports it to cflowd servers and packet analyzers. [Figure 20 on page 1124](#) shows a typical topology for the passive flow-monitoring application.

**Figure 20: Passive Monitoring Application Topology**



Traffic travels normally between Router 1 and Router 2. To redirect IPv4 traffic, you insert an optical splitter on the interface between these two routers. The optical splitter copies and redirects the traffic to the monitoring station, which is an M40e, M160, M320, or T Series router. The optical cable connects only the receive port on the monitoring station, never the transmit port. This configuration allows the monitoring station to receive traffic from the router being monitored but never to transmit it back.

If you are monitoring traffic flow, the Internet Processor II application-specific integrated circuit (ASIC) in the router forwards a copy of the traffic to the Monitoring Services, Adaptive Services, or Multiservices PIC in the monitoring station. If more than one monitoring PIC is installed, the monitoring station distributes the load of the incoming traffic across the multiple PICs. The monitoring PICs generate flow records in cflowd version 5 format, and the records are then exported to the cflowd collector.

If you are performing lawful interception of traffic between the two routers, the Internet Processor II ASIC filters the incoming traffic and forwards it to the Tunnel Services PIC. Filter-based forwarding is then applied to direct the traffic to the packet analyzers.

Optionally, the intercepted traffic or the cflowd records can be encrypted by the ES PIC or IP Security (IPsec) services and then sent to a cflowd server or packet analyzer.

#### Related Documentation

- [Enabling Passive Flow Monitoring on page 1203](#)

## Active Flow Monitoring Overview

Using a Juniper Networks M Series Multiservice Edge or T Series Core Router or EX9200 switch, a selection of PICs (including the Monitoring Services PIC, Adaptive Services [AS] PIC, Multiservices PIC, or Multiservices DPC) and other networking hardware, you can monitor traffic flow and export the monitored traffic. Monitoring traffic allows you to do the following:

- Gather and export detailed information about IP version 4 (IPv4) traffic flows between source and destination nodes in your network.
- Sample all incoming IPv4 traffic on the monitoring interface and present the data in cflowd record format.
- Perform discard accounting on an incoming traffic flow.
- Encrypt or tunnel outgoing cflowd records, intercepted IPv4 traffic, or both.
- Direct filtered traffic to different packet analyzers and present the data in its original format (port mirror).



**NOTE:** Monitoring Services PICs, AS PICs, and Multiservices PICs must be mounted on an Enhanced Flexible PIC Concentrator (FPC) in an M Series or T Series router.

Multiservices DPCs installed in Juniper Networks MX Series 3D Universal Edge Routers support the same functionality, with the exception of the passive monitoring and flow-tap features.

Although the Monitoring Services PIC was designed initially for use as an offline passive flow monitoring tool, it can also be used in an active flow monitoring topology. In contrast, the AS or Multiservices PIC is designed exclusively for active flow monitoring. To use either the Monitoring Services PIC, AS PIC, or Multiservices PIC for active flow monitoring, you must install the PIC in an M Series or T Series router. The router participates in both the monitoring application and in the normal routing functionality of the network.

Starting with Junos OS Release 11.4, support for active monitoring is extended to logical systems running on T Series and MX Series routers. A logical system is a partition created from a physical router that performs independent routing tasks. Several logical systems in a single router with their own interfaces, policies, instances, and routing tables can perform functions handled by several different routers. A shared services PIC handles flows from all the logical systems. Only version 9 flows, IPv4, and MPLS templates are supported. See [“Example: Configuring Active Monitoring on Logical Systems” on page 1148](#) for a sample configuration that enables active monitoring on a logical system.

Specified packets can be filtered and sent to the monitoring interface. For the Monitoring Services PIC, the interface name contains the **mo-** prefix. For the AS or Multiservices PIC, the interface name contains the **sp-** prefix.



**NOTE:** If you upgrade from the Monitoring Services PIC to the Adaptive Services or Multiservices PIC for active flow monitoring, you must change the name of your monitoring interface from **mo-fpc/pic/port** to **sp-fpc/pic/port**.

The major active flow monitoring actions you can configure at the **[edit forwarding-options]** hierarchy level are as follows:

- Sampling, with the **[edit forwarding-options sampling]** hierarchy. This option sends a copy of the traffic stream to an AS or Monitoring Services PIC, which extracts limited information (such as the source and destination IP address) from some of the packets in a flow. The original packets are forwarded to the intended destination as usual.
- Discard accounting, with the **[edit forwarding-options accounting]** hierarchy. This option quarantines unwanted packets, creates cflowd records that describe the packets, and discards the packets instead of forwarding them.
- Port mirroring, with the **[edit forwarding-options port-mirroring]** hierarchy. This option makes one full copy of all packets in a flow and delivers the copy to a single destination. The original packets are forwarded to the intended destination.
- Multiple port mirroring, with the **[edit forwarding-options next-hop-group]** hierarchy. This option allows multiple copies of selected traffic to be delivered to multiple destinations. (Multiple port mirroring requires a Tunnel Services PIC.)

Unlike passive flow monitoring, you do not need to configure a monitoring group. Instead, you can send filtered packets to a monitoring services or adaptive services interface (**mo-** or **sp-**) by using sampling or discard accounting. Optionally, you can configure port mirroring or multiple port mirroring to direct packets to additional interfaces.

These active flow monitoring options provide a wide variety of actions that can be performed on network traffic flows. However, the following restrictions apply:

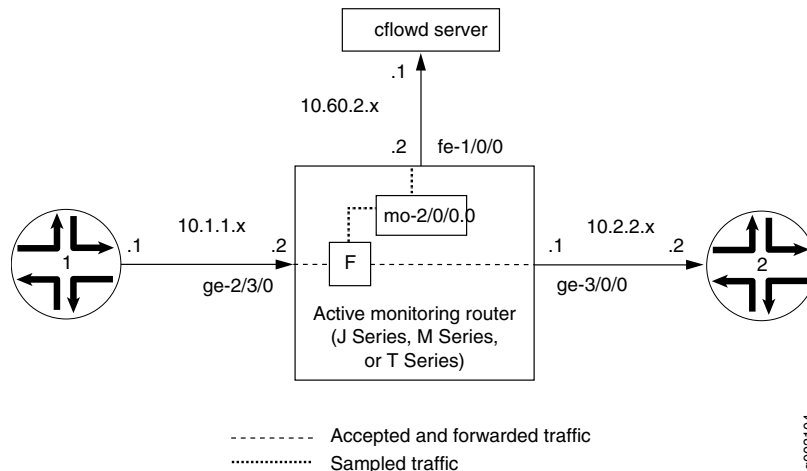
- The router or switch can perform sampling or port mirroring at any one time.
- The router or switch can perform forwarding or discard accounting at any one time.

Because the Monitoring Services, AS, and Multiservices PICs allow only one action to be performed at any one time, the following configuration options are available:

- Sampling and forwarding
- Sampling and discard accounting
- Port mirroring and forwarding
- Port mirroring and discard accounting
- Sampling and port mirroring on different sets of traffic

Figure 21 on page 1127 shows a sample topology.

Figure 21: Active Monitoring Configuration Topology



In Figure 21 on page 1127, traffic from Router 1 arrives on the monitoring router's Gigabit Ethernet **ge-2/3/0** interface. The exit interface on the monitoring router leading to destination Router 2 is **ge-3/0/0**, but this could be any interface type (such as SONET, Gigabit Ethernet, and so on). The export interface leading to the cflowd server is **fe-1/0/0**.

To enable active monitoring, configure a firewall filter on the interface **ge-2/3/0** with the following match conditions:

- Traffic matching certain firewall conditions is sent to the Monitoring Services PIC using filter-based forwarding. This traffic is quarantined and not forwarded to other routers.
- All other traffic is port-mirrored to the Monitoring Services PIC. Port mirroring copies each packet and sends the copies to the port-mirroring next hop (in this case, a Monitoring Services PIC). The original packets are forwarded out of the router as usual.

**Related  
Documentation**

- [Configuring Flow Monitoring on page 1144](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 1182](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 1210](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 1148](#)

# Flow Monitoring and Discard Accounting Configuration Guidelines

To configure flow monitoring and accounting interfaces, include the following statements at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
mo-fpc/pic/port {
  unit logical-unit-number {
    family inet {
      accounting {
        destination-class-usage;
        source-class-usage direction;
      }
    }
    address address {
      destination address;
    }
    filter {
      group filter-group-number;
      input filter-name;
      output filter-name;
    }
    receive-options-packets;
    receive-ttl-exceeded;
    sampling direction;
  }
}
multiservice-options {
  (core-dump | no-core-dump);
  (syslog | no-syslog);
  flow-control-options {
    down-on-flow-control;
    dump-on-flow-control;
    reset-on-flow-control;
  }
}
(at-fpc/pic/port | fe-fpc/pic/port | ge-fpc/pic/port) {
  passive-monitor-mode;
}
so-fpc/pic/port {
  unit logical-unit-number {
```

```

    passive-monitor-mode;
  }
}

```

To configure flow monitoring and accounting properties, include the following statements at the **[edit forwarding-options]** hierarchy level:

```

[edit forwarding-options]
accounting name {
  output {
    aggregate-export-interval seconds;
    cflowd hostname {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
    }
    autonomous-system-type (origin | peer);
    port port-number;
    version format;
  }
  flow-active-timeout seconds;
  flow-inactive-timeout seconds;
  interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
  }
}
}
monitoring name {
  family family {
    output {
      cflowd hostname port port-number;
      export-format format;
      flow-active-timeout seconds;
      flow-export-destination {
        collector-pic;
      }
      flow-inactive-timeout seconds;
      interface interface-name {
        engine-id number;
        engine-type number;
        input-interface-index number;
        output-interface-index number;
        source-address address;
      }
    }
  }
}
next-hop-group group-names {
  interface interface-name {
    next-hop address;
  }
}

```

```

    }
  }
  port-mirroring {
    input {
      rate rate;
      run-length number;
      maximum-packet-length bytes
    }
    family (inet | inet6) {
      output {
        interface interface-name {
          next-hop address;
        }
        no-filter-check;
      }
    }
  }
  traceoptions {
    file filename {
      files number;
      size bytes;
      (world-readable | no-world-readable);
    }
  }
}
sampling {
  disable;
  sample-once;
  input {
    rate number;
    run-length number;
    max-packets-per-second number;
    maximum-packet-length bytes;
  }
  traceoptions {
    no-remote-trace;
    file filename <files number> <size bytes> <match expression> <world-readable |
      no-world-readable>;
  }
}
family (inet | inet6 | mpls) {
  disable;
  output {
    aggregate-export-interval seconds;
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    extension-service service-name;
    flow-server hostname {
      aggregation {
        autonomous-system;
        destination-prefix;
        protocol-port;
        source-destination-prefix {
          caida-compliant;
        }
        source-prefix;
      }
      autonomous-system-type (origin | peer);
    }
  }
}

```

```

        (local-dump | no-local-dump);
        port port-number;
        source-address address;
        version format;
        version9 {
            template template-name;
        }
    }
}
interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
}
file {
    disable;
    filename filename;
    files number;
    size bytes;
    (stamp | no-stamp);
    (world-readable | no-world-readable);
}
}
instance instance-name {
    disable;
    input {
        rate number;
        run-length number;
        max-packets-per-second number;
        maximum-packet-length bytes;
    }
    family (inet | inet6 | mpls) {
        disable;
        output {
            aggregate-export-interval seconds;
            flow-active-timeout seconds;
            flow-inactive-timeout seconds;
            extension-service service-name;
            flow-server hostname {
                aggregation {
                    autonomous-system;
                    destination-prefix;
                    protocol-port;
                    source-destination-prefix {
                        caida-compliant;
                    }
                    source-prefix;
                }
            }
            autonomous-system-type (origin | peer);
            (local-dump | no-local-dump);
            port port-number;
            source-address address;
            version format;
            version9 {
                template template-name;
            }
        }
    }
}

```

```

}
interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
}
inline-jflow {
    source-address address;
    flow-export-rate rate;
}
}
}
}
}
}

```



**NOTE:** For the complete [edit forwarding-options] hierarchy, see the *Routing Policy Feature Guide for Routing Devices*. This section documents only the statements used in flow monitoring and accounting services.

To configure flow monitoring that uses cflowd version 9, include the following statements at the [edit services] hierarchy level:

```

[edit services]
flow-monitoring {
    version9 {
        template template-name {
            options-template-id
            template-id
            source-id
            flow-active-timeout seconds;
            flow-inactive-timeout seconds;
            ipv4-template;
            ipv6-template;
            mpls-template {
                label-position [ positions ];
            }
            mpls-ipv4-template {
                label-position [ positions ];
            }
            peer-as-billing-template;
            option-refresh-rate packets packets seconds seconds;
            template-refresh-rate packets packets seconds seconds;
        }
    }
}

```

This chapter contains the following sections:

- [Configuring Traffic Sampling on page 1134](#)
- [Configuring Flow Monitoring on page 1144](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 1148](#)
- [Enabling Flow Aggregation on page 1151](#)

- [Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd on page 1152](#)
- [Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156](#)
- [Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 1167](#)
- [Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows on page 1172](#)
- [Sampling Instance Configuration on page 1175](#)
- [Configuring Inline Sampling on page 1176](#)
- [Configuring Inline Sampling on MX80 Routers on page 1181](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 1182](#)
- [Logging cflowd Flows Before Export on page 1185](#)
- [Configuring Port Mirroring on page 1186](#)
- [Load Balancing Among Multiple Monitoring Interfaces on page 1199](#)
- [Configuring Discard Accounting on page 1202](#)
- [Enabling Passive Flow Monitoring on page 1203](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 1210](#)

## Configuring Traffic Sampling

---

Traffic sampling enables you to copy traffic to a Physical Interface Card (PIC) that performs flow accounting while the router forwards the packet to its original destination. You can configure the router to perform sampling in either of two locations:

- On the Routing Engine, using the sampled process. To select this method, use a filter (input or output) with a matching term that contains the **then sample** statement.
- On the Monitoring Services, Adaptive Services, or Multiservices PIC.



.....

**NOTE:** Routing Engine based sampling is not supported on VPN routing and forwarding (VRF) instances.

.....

The following sections provide configuration instructions for traffic sampling:

- [Configuring Firewall Filter for Traffic Sampling on page 1135](#)
- [Configuring Traffic Sampling on a Logical Interface on page 1136](#)
- [Disabling Traffic Sampling on page 1137](#)
- [Sampling Once on page 1137](#)
- [Preserving Prerewrite ToS Value for Egress Sampled or Mirrored Packets on page 1137](#)
- [Configuring Traffic Sampling Output on page 1138](#)
- [Tracing Traffic Sampling Operations on page 1140](#)
- [Traffic Sampling Examples on page 1141](#)

## Configuring Firewall Filter for Traffic Sampling

To configure firewall filter for traffic sampling, you must perform the following tasks:

- Create a firewall filter to apply to the logical interfaces being sampled by including the **filter** statement at the **[edit firewall family *family-name*]** hierarchy level. In the filter **then** statement, you must specify the action modifier **sample** and the action **accept**.

```
filter filter-name {
  term term-name {
    then {
      sample;
      accept;
    }
  }
}
```

For more information about firewall filter actions and action modifiers, see the *Routing Policy Feature Guide for Routing Devices*.

- Apply the filter to the interfaces on which you want to sample traffic by including the **address** and **filter** statements at the **[edit interfaces *interface-name* unit *logical-unit-number* family *family-name*]** hierarchy level:

```
address address {
}
filter {
  input filter-name;
}
```

The following prerequisites apply to M, MX, and T Series routers when you configure traffic sampling on interfaces and in firewall filters:

- If you configure a sample action in a firewall filter for an inet or inet6 family on an interface without configuring the forwarding-options settings, operational problems might occur if you also configure port mirroring or flow-tap functionalities. In such a scenario, all the packets that match the firewall filter are incorrectly sent to the service PIC.
- If you include the **then sample** statement at the **[edit firewall family inet filter *filter-name* term *term-name*]** hierarchy level to specify a sample action in a firewall filter for IPv4 packets, you must also include the **family inet** statement at the **[edit forwarding-options sampling]** hierarchy level or the **instance *instance-name* family inet** statement at the **[edit forwarding-options sampling]** hierarchy level. Similarly, if you include the **then sample** statement at the **[edit firewall family inet6 filter *filter-name* term *term-name*]** hierarchy level to specify a sample action in a firewall filter for IPv6 packets, you must also include **family inet6** statement at the **[edit forwarding-options sampling]** hierarchy level or the **instance *instance-name* family inet6** statement at the **[edit forwarding-options sampling]** hierarchy level. Otherwise, a commit error occurs when you attempt to commit the configuration.
- Also, if you configure traffic sampling on a logical interface by including the sampling input or sampling output statements at the **[edit interface *interface-name* unit**

**logical-unit-number**] hierarchy level, you must also include the **family inet | inet6** statement at the **[edit forwarding-options sampling]** hierarchy level, or the **instance instance-name family inet | inet6** statement at the **[edit forwarding-options sampling]** hierarchy level.

## Configuring Traffic Sampling on a Logical Interface

To configure traffic sampling on any logical interface, enable sampling and specify a non zero sampling rate by including the sampling statement at the **[edit forwarding-options]** hierarchy level:

```
sampling {
  input {
    rate number;
    run-length number;
    max-packets-per-second number;
    maximum-packet-length bytes;
  }
}
```

When you use Routing Engine-based sampling, specify the threshold traffic value by including the **max-packets-per-second** statement. The value is the maximum number of packets to be sampled, beyond which the sampling mechanism begins dropping packets. The range is from 0 through 65,535. A value of 0 instructs the Packet Forwarding Engine not to sample any packets. The default value is 1000.



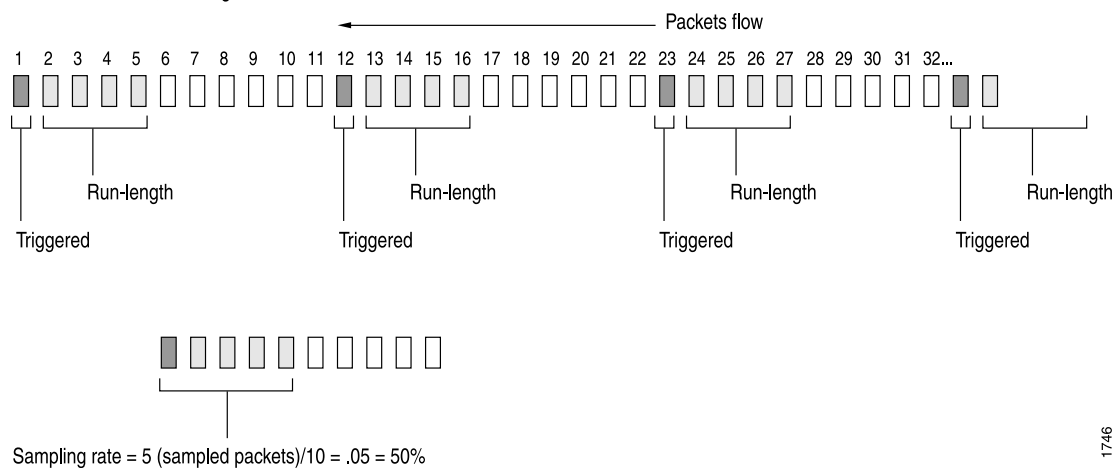
**NOTE:** When you configure active monitoring and specify a Monitoring Services, Adaptive Services, or Multiservices PIC in the output statement, the **max-packets-per-second** value is ignored.

Specify the sampling rate by setting the values for **rate** and **run-length** (see Figure 22 on page 1136).

**Figure 22: Configuring Sampling Rate**

### Rate and Run-length

Case #1 Rate =10, run-length =4



The **rate** statement specifies the ratio of packets to be sampled. For example, if you configure a rate of 10, x number of packets out of every 10 is sampled, where  $x = \text{run length} + 1$ . By default, the rate is 0, which means that no traffic is sampled.

The **run-length** statement specifies the number of matching packets to sample following the initial one-packet trigger event. By default, the run length is 0, which means that no more traffic is sampled after the trigger event. The range is from 0 through 20. Configuring a run length greater than 0 allows you to sample packets following those already being sampled.



**NOTE:** The **run-length** and **maximum-packet-length** configuration statements are not supported on MX80 routers.

If you do not include the **input** statement, sampling is disabled.

To collect the sampled packets in a file, include the **file** statement at the **[edit forwarding-options sampling output]** hierarchy level. Output file formats are discussed later in the chapter.

## Disabling Traffic Sampling

To explicitly disable traffic sampling on the router, include the **disable** statement at the **[edit forwarding-options sampling]** hierarchy level:

```
disable;
```

## Sampling Once

To explicitly sample a packet for active monitoring only once, include the **sample-once** statement at the **[edit forwarding-options sampling]** hierarchy level:

```
sample-once;
```

Setting this option avoids duplication of packets in cases where sampling is enabled at both the ingress and egress interfaces and simplifies analysis of the sampled traffic.

## Preserving Prerewrite ToS Value for Egress Sampled or Mirrored Packets

To preserve the prenormalized type-of-service (ToS) value in egress sampled or mirrored packets, include the **pre-rewrite-tos** statement at the **[edit forwarding-options sampling]** hierarchy level.

On MPC-based interfaces, you can configure ToS rewrite either using class-of-service (CoS) configuration by including the **rewrite-rules dscp rule\_name** statement at the **[edit class-of-service interfaces interface-name unit logical-unit-number]** hierarchy level or using firewall filter configuration by including the **dscp** statement at the **[edit firewall family family-name filter filter-name term term-name then]** hierarchy level. If ToS rewrite is configured, the egress mirrored or sampled copies contain the post-rewrite ToS values by default. With the **pre-rewrite-tos** configuration, you can retain the prerewrite ToS value in the sampled or mirrored packets.

**NOTE:**

- If ToS rewrite is configured on the egress interface by using both CoS and firewall filter configuration, and if the `pre-rewrite-tos` statement is also configured, then the egress sampled packets contain the DSCP value set using the firewall filter configuration. However, if the `pre-rewrite-tos` statement is not configured, the egress sampled packets contain the DSCP value set by the CoS configuration.
- With the `pre-rewrite-tos` statement, you can configure retaining prenormalization ToS values only for sampling done under family `inet` and family `inet6`.
- This feature cannot be configured at the `[edit logical-systems]` hierarchy level. It can be configured only at the global level under the `forwarding-option` configuration.
- When ToS rewrite is configured by using a firewall filter on both ingress and egress interfaces, the egress sampled packets contain the DSCP value set by the ingress ToS rewrite configuration if the `pre-rewrite-tos` statement is configured. However, if the `pre-rewrite-tos` statement is not configured, the egress sampled packets contain the DSCP value set by the ToS rewrite configuration for the egress firewall filter.
- If the `pre-rewrite-tos` statement is configured, and a deactivate or delete operation is performed at the `[edit forwarding-options]` hierarchy level, `pre-rewrite-tos` configuration still remains active. To disable the `pre-rewrite-tos` configuration for such a case, you must explicitly deactivate or delete the `pre-rewrite-tos` statement at the `[edit forwarding-options sampling]` hierarchy level before performing a deactivate or delete operation at the `[edit forwarding-options]` hierarchy level.

## Configuring Traffic Sampling Output

To configure traffic sampling output, include the following statements at the `[edit forwarding-options sampling family (inet | inet6 | mpls) output]` hierarchy level:

```

aggregate-export-interval seconds;
flow-active-timeout seconds;
flow-inactive-timeout seconds;
extension-service service-name;
flow-server hostname {
  aggregation {
    autonomous-system;
    destination-prefix;
    protocol-port;
    source-destination-prefix {
      caida-compliant;
    }
    source-prefix;
  }
  autonomous-system-type (origin | peer);
}

```

```

(local-dump | no-local-dump);
port port-number;
source-address address;
version format;
version9 {
    template template-name;
}
}
interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
}
file {
    disable;
    filename filename;
    files number;
    size bytes;
    (stamp | no-stamp);
    (world-readable | no-world-readable);
}

```

To configure inline flow monitoring on MX Series routers, include the **inline-jflow** statement at the **[edit forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls) output]** hierarchy level. Inline sampling exclusively supports a new format called IP\_FIX that uses UDP as the transport protocol. When you configure inline sampling, you must include the **version-ipfix** statement at the **[edit forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls) output flow-server address]** hierarchy level and also at the **[edit services flow-monitoring]** hierarchy level. For more information about configuring inline flow monitoring, see [“Configuring Inline Sampling” on page 1176](#).

To direct sampled traffic to a flow-monitoring interface, include the **interface** statement. The **engine-id** and **engine-type** statements specify the identity and type numbers of the interface; they are dynamically generated based on the Flexible PIC Concentrator (FPC), PIC, and slot numbers and the chassis type. The **source-address** statement specifies the traffic source.

To configure flow sampling version 9 output, you need to include the **template** statement at the **[edit forwarding-options sampling output version9]** hierarchy level. For information on cflowd, see [“Enabling Flow Aggregation” on page 1151](#).

The **aggregate-export-interval** statement is described in [“Configuring Discard Accounting” on page 1202](#), and the **flow-active-timeout** and **flow-inactive-timeout** statements are described in [“Configuring Flow Monitoring” on page 1144](#).

Traffic sampling results are automatically saved to a file in the **/var/tmp** directory. To collect the sampled packets in a file, include the **file** statement at the **[edit forwarding-options sampling family inet output]** hierarchy level:

```

file {
    disable;
    filename filename;
    files number;
    size bytes;
}

```

```
(stamp | no-stamp);
(world-readable | no-world-readable);
}
```

### Traffic Sampling Output Format

Traffic sampling output is saved to an ASCII text file. The following is an example of the traffic sampling output that is saved to a file in the **/var/tmp** directory. Each line in the output file contains information for one sampled packet. You can optionally display a timestamp for each line.

The column headers are repeated after each group of 1000 packets.

```
# Apr  7 15:48:50
Time                Dest                Src Dest Src Proto TOS Pkt Intf  IP    TCP
                  addr                addr port port
Apr 7 15:48:54 192.168.9.194 192.168.9.195 0  0  1  0x0 84 8  0x0 0x0
Apr 7 15:48:55 192.168.9.194 192.168.9.195 0  0  1  0x0 84 8  0x0 0x0
Apr 7 15:48:56 192.168.9.194 192.168.9.195 0  0  1  0x0 84 8  0x0 0x0
Apr 7 15:48:57 192.168.9.194 192.168.9.195 0  0  1  0x0 84 8  0x0 0x0
Apr 7 15:48:58 192.168.9.194 192.168.9.195 0  0  1  0x0 84 8  0x0 0x0
```

To set the timestamp option for the file **my-sample**, enter the following:

```
[edit forwarding-options sampling output file]
user@host# set filename my-sample files 5 size 2m world-readable stamp;
```

Whenever you toggle the timestamp option, a new header is included in the file. If you set the **stamp** option, the **Time** field is displayed.

```
# Apr  7 15:48:50
# Time                Dest                Src Dest Src Proto TOS  Pkt Intf  IP    TCP
#                   addr                addr port port      len  num frag flags
# Feb  1 20:31:21
#                   Dest                Src Dest Src Proto TOS  Pkt Intf  IP    TCP
#                   addr                addr port port      len  num frag flags
```

## Tracing Traffic Sampling Operations

Tracing operations track all traffic sampling operations and record them in a log file in the **/var/log** directory. By default, this file is named **/var/log/sampled**. The default file size is 128K, and 10 files are created before the first one gets overwritten.

To trace traffic sampling operations, include the **traceoptions** statement at the **[edit forwarding-options sampling]** hierarchy level:

```
traceoptions {
  no-remote-trace;
  file filename <files number> <size bytes> <match expression> <world-readable |
  no-world-readable>;
}
```

## Traffic Sampling Examples

The following sections provide examples of configuring traffic sampling:

- [Example: Sampling a Single SONET/SDH Interface on page 1141](#)
- [Example: Sampling All Traffic from a Single IP Address on page 1142](#)
- [Example: Sampling All FTP Traffic on page 1143](#)

### Example: Sampling a Single SONET/SDH Interface

The following configuration gathers statistical sampling information from a small percentage of all traffic on a single SONET/SDH interface and collects it in a file named **sonet-samples.txt**.

Create the filter:

```
[edit firewall family inet]
filter {
  input sample-sonet {
    then {
      sample;
      accept;
    }
  }
}
```

Apply the filter to the SONET/SDH interface:

```
[edit interfaces]
so-0/0/1 {
  unit 0 {
    family inet {
      filter {
        input sample-sonet;
      }
      address 10.127.68.254/32 {
        destination 172.16.74.7;
      }
    }
  }
}
```

Finally, configure traffic sampling:

```
[edit forwarding-options]
sampling {
  input {
    family inet {
      rate 100;
      run-length 2;
    }
  }
  family inet {
    output {
      file {
```

```
        filename sonet-samples.txt;
        files 40;
        size 5m;
    }
}
}
```

### Example: Sampling All Traffic from a Single IP Address

---

The following configuration gathers statistical information about every packet entering the router on a specific Gigabit Ethernet port originating from a single source IP address of **172.16.92.31**, and collects it in a file named **samples-172-16-92-31.txt**.

Create the filter:

```
[edit firewall family inet]
filter one-ip {
  term get-ip {
    from {
      source-address 172.16.92.31;
    }
    then {
      sample;
      accept;
    }
  }
}
```

Apply the filter to the Gigabit Ethernet interface:

```
[edit interfaces]
ge-4/1/1 {
  unit 0 {
    family inet {
      filter {
        input one-ip;
      }
      address 10.45.92.254;
    }
  }
}
```

Finally, gather statistics on all the candidate samples; in this case, gather all statistics:

```
[edit forwarding-options]
sampling {
  input {
    family inet {
      rate 1;
    }
  }
  family inet {
    output {
      file {
        filename samples-172-16-92-31.txt;
        files 100;
      }
    }
  }
}
```

```

        size 100k;
    }
}
}

```

### Example: Sampling All FTP Traffic

The following configuration gathers statistical information about a moderate percentage of packets using the FTP data transfer protocol in the output path of a specific T3 interface, and collects the information in a file named **t3-ftp-traffic.txt**.

Create a filter:

```

[edit firewall family inet]
filter ftp-stats {
  term ftp-usage {
    from {
      destination-port [ftp ftp-data];
    }
    then {
      sample;
      accept;
    }
  }
}

```

Apply the filter to the T3 interface:

```

[edit interfaces]
t3-7/0/2 {
  unit 0 {
    family inet {
      filter {
        input ftp-stats;
      }
      address 10.35.78.254/32 {
        destination 10.35.78.4;
      }
    }
  }
}

```

Finally, gather statistics on 10 percent of the candidate samples:

```

[edit forwarding-options]
sampling {
  input {
    family inet {
      rate 10;
    }
  }
  family inet {
    output {
      file {
        filename t3-ftp-traffic.txt;
        files 50;
      }
    }
  }
}

```

```
        size 1m;
      }
    }
  }
}
```

- Related Documentation**
- [Traffic Sampling, Forwarding, and Monitoring Overview](#)
  - [Sampling Instance Configuration on page 1175](#)

---

## Configuring Flow Monitoring

The flow-monitoring application performs traffic flow monitoring and enables lawful interception of traffic between two routers or switches. Traffic flows can either be passively monitored by an offline router or switch or actively monitored by a router participating in the network.

To configure flow monitoring you need to do the following:

- [Configuring Flow-Monitoring Interfaces on page 1144](#)
- [Configuring Flow-Monitoring Properties on page 1145](#)
- [Example: Configuring Flow Monitoring on page 1147](#)

### Configuring Flow-Monitoring Interfaces

To enable flow monitoring on the Monitoring Services PIC, include the **mo-fpc/pic/port** statement at the **[edit interfaces]** hierarchy level:

```
mo-fpc/pic/port {
  unit logical-unit-number {
    family inet {
      address address {
        destination address;
      }
      filter {
        group filter-group-number;
        input filter-name;
        output filter-name;
      }
      sampling {
        [ input output ];
      }
    }
  }
  multiservice-options {
    (core-dump | no-core-dump);
    (syslog | no-syslog);
    flow-control-options {
      down-on-flow-control;
      dump-on-flow-control;
      reset-on-flow-control;
    }
  }
}
```

```
}
```

Specify the physical and logical location of the flow-monitoring interface. You cannot use **unit 0**, because it is already used by internal processes. Specify the source and destination addresses. The **filter** statement allows you to associate an input or output filter or a filter group that you have already configured for this purpose. The **sampling** statement specifies the traffic direction: **input**, **output**, or both.

The **multiservice-options** statement allows you to configure properties related to flow-monitoring interfaces:

- Include the **core-dump** statement to enable storage of core files in **/var/tmp**.
- Include the **syslog** statement to enable storage of system logging information in **/var/log**.



**NOTE:** Boot images for monitoring services interfaces are specified at the **[edit chassis images pic]** hierarchy level. You must include the following configuration to make the flow monitoring feature operable:

```
[edit system]
ntp {
  boot-server ntp.juniper.net;
  server 172.17.28.5;
}
processes {
  ntp enable;
}
```

For more information, see the *Junos OS Administration Library for Routing Devices*.

- Include the **flow-control-options** statement to configure flow control.

## Configuring Flow-Monitoring Properties

To configure flow-monitoring properties, include the **monitoring** statement at the **[edit forwarding-options]** hierarchy level:

```
monitoring name {
  family inet {
    output {
      cflowd hostname port port-number;
      export-format format;
      flow-active-timeout seconds;
      flow-export-destination {
        collector-pic;
      }
      flow-inactive-timeout seconds;
    }
    interface interface-name {
      engine-id number;
      engine-type number;
      input-interface-index number;
    }
  }
}
```

```
        output-interface-index number;  
        source-address address;  
    }  
}  
}
```

A monitoring instance is a named entity that specifies collector information under the **monitoring *name*** statement. The following sections describe the properties you can configure:

- [Directing Traffic to Flow-Monitoring Interfaces on page 1146](#)
- [Exporting Flows on page 1146](#)
- [Configuring Time Periods when Flow Monitoring is Active and Inactive on page 1147](#)

---

### Directing Traffic to Flow-Monitoring Interfaces

To direct traffic to a flow-monitoring interface, include the **interface** statement at the **[edit forwarding-options monitoring *name* output]** hierarchy level. By default, the Junos OS automatically assigns values for the **engine-id** and **engine-type** statements:

- **engine-id**—Monitoring interface location.
- **engine-type**—Platform-specific monitoring interface type.

The **source-address** statement specifies the traffic source for transmission of cflowd information; you must configure it manually. If you provide a different **source-address** statement for each monitoring services output interface, you can track which interface processes a particular cflowd record.

By default, the **input-interface-index** value is the SNMP index of the input interface. You can override the default by including a specific value. The **input-interface-index** and **output-interface-index** values are exported in fields present in the cflowd version 5 flow format.



**NOTE:** On J Series Services Routers, cflowd sampling in the input direction of an interface reports the output interface index as 0.

---

---

### Exporting Flows

To direct traffic to a flow collection interface, include the **flow-export-destination** statement. For more information about flow collection, see *Flow Collection*.

To configure the cflowd version number, include the **export-format** statement at the **[edit forwarding-options monitoring *name* output]** hierarchy level. By default, version 5 is used. Version 8 enables the router software to aggregate the flow information using broader criteria and reduce cflowd traffic. Version 8 aggregation is performed periodically (every few seconds) on active flows and when flows are allowed to expire. Because the aggregation is performed periodically, active timeout events are ignored.

For more information on cflowd properties, see [“Enabling Flow Aggregation” on page 1151](#).

### Configuring Time Periods when Flow Monitoring is Active and Inactive

To configure time periods for active flow monitoring and intervals of inactivity, include the **flow-active-timeout** and **flow-inactive-timeout** statements at the **[edit forwarding-options monitoring *name* output]** hierarchy level:

- The **flow-active-timeout** statement specifies the time interval between flow exports for active flows. If the interval between the time the last packet was received and the time the flow was last exported exceeds the configured value, the flow is exported.

This timer is needed to provide periodic updates when a flow has a long duration. The active timeout setting enables the router to retain the start time for the flow as a constant and send out periodic cflowd reports. This in turn allows the collector to register the start time and determine that a flow has survived for a duration longer than the configured active timeout.



**NOTE:** In active flow monitoring, the cflowd records are exported after a time period that is a multiple of 60 seconds and greater than or equal to the configured active timeout value. For example, if the active timeout value is 90 seconds, the cflowd records are exported at 120-second intervals. If the active timeout value is 150 seconds, the cflowd records are exported at 180-second intervals, and so forth.

- The **flow-inactive-timeout** statement specifies the interval of inactivity for a flow that triggers the flow export. If the interval between the current time and the time that the last packet for this flow was received exceeds the configured inactive timeout value, the flow is allowed to expire.

If the flow stops transmitting for longer than the configured inactive timeout value, the router or switch purges it from the flow table and exports the cflowd record. As a result, the flow is forgotten as far as the PIC is concerned and if the same 5-tuple appears again, it is assigned a new start time and considered a new flow.

Both timers are necessary. The active timeout setting is needed to provide information for flows that constantly transmit packets for a long duration. The inactive timeout setting enables the router or switch to purge flows that have become inactive and would waste tracking resources.



**NOTE:** The router must contain an Adaptive Services, Multiservices, or Monitoring Services PIC for the **flow-active-timeout** and **flow-inactive-timeout** statements to take effect.

### Example: Configuring Flow Monitoring

The following is an example of flow-monitoring properties configured to support input SONET/SDH interfaces, output monitoring services interfaces, and export to cflowd for flow analysis. To complete the configuration, you also need to configure the interfaces and set up a virtual private network (VPN) routing and forwarding (VRF) instance. For a

complete example, see the *Junos OS, Release 14.1*. For information on cflowd, see [“Enabling Flow Aggregation” on page 1151](#).

```
[edit forwarding-options]
monitoring group1 {
  family inet {
    output {
      cflowd 192.168.245.2 port 2055;
      export-format cflowd-version-5;
      flow-active-timeout 60;
      flow-inactive-timeout 30;
      interface mo-4/0/0.1 {
        engine-id 1;
        engine-type 1;
        input-interface-index 44;
        output-interface-index 54;
        source-address 192.168.245.1;
      }
      interface mo-4/1/0.1 {
        engine-id 2;
        engine-type 1;
        input-interface-index 45;
        output-interface-index 55;
        source-address 192.168.245.1;
      }
      interface mo-4/2/0.1 {
        engine-id 3;
        engine-type 1;
        input-interface-index 46;
        output-interface-index 56;
        source-address 192.168.245.1;
      }
      interface mo-4/3/0.1 {
        engine-id 4;
        engine-type 1;
        input-interface-index 47;
        output-interface-index 57;
        source-address 192.168.245.1;
      }
    }
  }
}
```

**Related  
Documentation**

- [Active Flow Monitoring Overview on page 1125](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 1182](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 1210](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 1148](#)

---

## Example: Configuring Active Monitoring on Logical Systems

This example shows a sample configuration that allows you to configure active monitoring on a logical system. The following section shows the configuration on the master router:

```
[edit forwarding-options]
sampling {
  instance inst1 {
    input {
      rate 1;
    }
    family inet;
    output {
      flow-server 2.2.2.2 {
        port 2055;
        version9 {
          template {
            ipv4;
          }
        }
      }
    }
    interface sp-0/1/0 {
      source-address 10.11.12.13;
    }
  }
}
family mpls;
output {
  flow-server 2.2.2.2 {
    port 2055;
    version9 {
      template {
        mpls;
      }
    }
  }
}
interface sp-0/1/0 {
  source-address 10.11.12.13;
}
}
services {
  flow-monitoring {
    version9 {
      template ipv4 {
        flow-active-timeout 60;
        flow-inactive-timeout 60;
        ipv4-template;
        template-refresh-rate {
          packets 1000;
          seconds 10;
        }
        option-refresh-rate {
          packets 1000;
          seconds 10;
        }
      }
    }
    template mpls {
      mpls-template;
    }
  }
}
```

```

    }
  }
}

```

The configuration for the logical router uses the input parameters and the output interface for sampling from the master router. Each logical router should have separate template definitions for the flow-server configuration. The following section shows the configuration on the logical router:

```

logical-systems {
  ls-1 {
    firewall {
      family inet {
        filter test-sample {
          term term-1 {
            then {
              sample;
              accept;
            }
          }
        }
      }
    }
    interfaces {
      ge-0/0/1 {
        unit 0 {
          family inet {
            filter {
              input test-sample;
              output test-sample;
            }
          }
        }
      }
    }
    forwarding-options {
      sampling {
        instance sample-inst1 {
          family inet;
          output {
            flow-server 2.2.2.2 {
              port 2055;
              version9 {
                template {
                  ipv4-ls1;
                }
              }
            }
          }
        }
      }
    }
    family mpls;
    output {
      flow-server 2.2.2.2 {
        port 2055;
      }
    }
  }
}

```

**Related Documentation**

- [Active Flow Monitoring Overview on page 1125](#)
- [Configuring Flow Monitoring on page 1144](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 1182](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 1210](#)

- At the **[edit forwarding-options]** hierarchy level (for routing instances, at the **[edit routing-instance *routing-instance-name* forwarding-options]** hierarchy level), configure **sampling family** or **sampling output** or **sampling instance** or **monitoring** or **accounting**.

- At the `[edit routing-options]` hierarchy level (for routing instances, at the `[edit routing-instance routing-instance-name routing-options]` hierarchy level), configure `route record`.
- At the `[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]` hierarchy level, configure `forwarding-db-size`.

**Related  
Documentation**

- [Understanding Flow Aggregation](#)
- [Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd on page 1152](#)
- [Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 1182](#)
- [Configuring Traffic Sampling on page 1134](#)
- [Example: Configuring Active Flow Monitoring Version 9 for IPv6](#)
- [Logging cflowd Flows Before Export on page 1185](#)

---

## Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd

To enable the collection of cflowd version 5 or version 8 flow formats, include the `flow-server` statement:

```
flow-server hostname {
  aggregation {
    autonomous-system;
    destination-prefix;
    protocol-port;
    source-destination-prefix {
      caida-compliant;
    }
    source-prefix;
  }
  autonomous-system-type (origin | peer);
  (local-dump | no-local-dump);
  port port-number;
  version format;
}
```

You can include this statement at the following hierarchy levels:

- `[edit forwarding-options sampling family (inet | inet6 | mpls) output]`
- `[edit forwarding-options sampling instance instance-name output]`
- `[edit forwarding-options accounting name output cflowd hostname]`

You must configure the `family inet` statement on logical interface `unit 0` on the monitoring interface, as in the following example:

```
[edit interfaces]
sp-3/0/0 {
  unit 0 {
```

```

family inet {
    ...
}
}

```



**NOTE:** Boot images for monitoring services interfaces are specified at the `[edit chassis images pic]` hierarchy level. You must enable the NTP client to make the cflowd feature operable, by including the following configuration:

```

[edit system]
ntp {
    boot-server ntp.juniper.net;
    server 172.17.28.5;
}
processes {
    ntp enable;
}

```

For more information, see the *Junos OS Administration Library for Routing Devices*.

You can also configure cflowd version 5 for flow-monitoring applications by including the `cflowd` statement at the `[edit forwarding-options monitoring name family inet output]` hierarchy level:

```

cflowd hostname {
    port port-number;
}

```

The following restrictions apply to cflowd flow formats:

- You can configure up to one version 5 and one version 8 flow format at the `[edit forwarding-options accounting name output]` hierarchy level.
- You can configure up to eight version 5 or one version 8 flow format at the `[edit forwarding-options sampling family (inet | inet6 | mpls) output]` hierarchy level for Routing Engine-based sampling by including the `flow-server` statement. In contrast, PIC-based sampling allows you to specify one cflowd version 5 server and one version 8 server simultaneously. However, the two cflowd servers must have different IP addresses.
- You can configure up to eight version 5 flow formats at the `[edit forwarding-options monitoring name output]` hierarchy level. Version 8 flow formats and aggregation are not supported for flow-monitoring applications.
- Outbound Routing Engine traffic is not sampled. A firewall filter is applied as output on the egress interface, which samples packets and exports the data. For transit traffic, egress sampling works correctly. For internal traffic, the next hop is installed in the Packet Forwarding Engine but sampled packets are not exported.

- Flows are created on the monitoring PIC only after the route record resynchronization operation is complete, which is 60 seconds after the PIC comes up. Any packets sent to the PIC would be dropped until the synchronization process is complete.
- The configuration includes a proprietary v5 extension template for supporting 4-byte AS information in flow records. Its template version is set to 500, indicating it to be proprietary. All other fields remain the same; the source AS and destination AS are each 4 bytes long, rather than 2 bytes as in the traditional v5 template. This option is available at the `[edit forwarding-options sampling family inet output flow-server server-name version]` hierarchy level.

In the **cflowd** statement, specify the name or identifier of the host that collects the flow aggregates. You must also include the User Datagram Protocol (UDP) port number on the host and the version, which gives the format of the exported cflowd aggregates. To collect cflowd records in a log file before exporting, include the **local-dump** statement.



**NOTE:** You can specify both host (cflowd) sampling and port mirroring in the same configuration; however, only one action takes effect at any one time. Port mirroring takes precedence. For more information, see [“Configuring Port Mirroring” on page 1186](#).

For cflowd version 8 only, you can specify aggregation of specific types of traffic by including the **aggregation** statement. This conserves memory and bandwidth by enabling cflowd to export targeted flows rather than all aggregated traffic. To specify a flow type, include the **aggregation** statement:

```
aggregation {  
  autonomous-system;  
  destination-prefix;  
  protocol-port;  
  source-destination-prefix {  
    caida-compliant;  
  }  
  source-prefix;  
}
```

You can include this statement at the following hierarchy levels:

- `[edit forwarding-options sampling family (inet | inet6 | mpls) output flow-server hostname]`
- `[edit forwarding-options accounting name output cflowd hostname]`

The **autonomous-system** statement configures aggregation by the AS number; this statement might require setting the separate cflowd **autonomous-system-type** statement to include either **origin** or **peer** AS numbers. The **origin** option specifies to use the origin AS of the packet source address in the Source Autonomous System cflowd field. The **peer** option specifies to use the peer AS through which the packet passed in the Source Autonomous System cflowd field. By default, cflowd exports the origin AS number.

The **destination-prefix** statement configures aggregation by the destination prefix only.

The **protocol-port** statement configures aggregation by the protocol and port number; requires setting the separate **cflowd port** statement.

The **source-destination-prefix** statement configures aggregation by the source and destination prefix. Version 2.1b1 of CAIDA's cflowd application does not record source and destination mask length values in compliance with CAIDA's *cflowd Configuration Guide*, dated August 30, 1999. If you configure the **caida-compliant** statement, the Junos OS complies with Version 2.1b1 of cflowd. If you do not include the **caida-compliant** statement in the configuration, the Junos OS records source and destination mask length values in compliance with the *cflowd Configuration Guide*.

The **source-prefix** statement configures aggregation by the source prefix only.

Collection of sampled packets in a local ASCII file is not affected by the **cflowd** statement.

The following commands enable RE- and PIC-based sampling at the **set forwarding options sampling** hierarchy level:

- **set input rate** *rate*
- **set input run-length** *length*
- **set family inet output flow-server** *flowcollector* port *udp port*
- **set family inet output flow-server** *flowcollector* no-local-dump
- **set family inet output flow-server** *flowcollector* version <5/8>

The following commands enable RE- and PIC-based sampling at the **set interfaces** hierarchy level:

- **interface to be sampled** unit *unit* family inet filter *input/output filename*

The following commands enable RE- and PIC-based sampling at the **set firewall family** hierarchy level:

- **set inet filter** *filename* term 1 then count *filename* *ing*
- **set inet filter** *filename* term 1 then sample
- **set inet filter** *filename* term 1 then accept

The following command enables PIC-based sampling at the **set forwarding options sampling** hierarchy level:

- **set family inet output interface** *sp-\*/\*/\** source address *source address*

The following example shows a PIC-based flow aggregation configuration using version 5:

```
family inet {
  output {
    flow-inactive-timeout 15;
    flow-active-timeout 60;
    flow-server 153.104.248.37 {
      port 9996;
    }
  }
}
```

```
        version 5;
    }
    interface sp-2/2/0 {
        engine-id 4;
        source-address 153.104.0.254;
    }
}
```

The following example shows an RE-based flow aggregation configuration using version 5:

```
family inet {
    output {
        flow-inactive-timeout 15;
        flow-active-timeout 60;
        flow-server 153.104.248.37 {
            port 9996;
            source-address 153.104.0.254;
            version 5;
        }
    }
}
```

**Related  
Documentation**

- [Understanding Flow Aggregation](#)
- [Enabling Flow Aggregation on page 1151](#)
- [Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156](#)
- [Configuring Flow Aggregation to Use IPFIX Flow Templates](#)

---

## Configuring Flow Aggregation to Use Version 9 Flow Templates

---

Use of version 9 allows you to define a flow record template suitable for IPv4 traffic, IPv6 traffic, MPLS traffic, a combination of IPv4 and MPLS traffic, or peer AS billing traffic. Templates and the fields included in the template are transmitted to the collector periodically, and the collector need not be aware of the router configuration.



**NOTE:** Version 9 requires that you install a services PIC, such as the Adaptive Services PIC or Multiservices PIC in the router. On MX Series routers, the Multiservices DPC fulfills this requirement. For more information on determining which services PIC is suitable for your router, see [“Enabling Service Packages” on page 41](#) or the appropriate hardware documentation.



**NOTE:** If multiple protocol families are configured for a particular flow collector, the export packets will originate from multiple Source IDs, with each Source ID corresponding to a particular protocol. The multiple Source IDs do not indicate that the export packets are originating from multiple Service PICs.

The following sections contain additional information:

- [Configuring the Traffic to Be Sampled on page 1157](#)
- [Configuring the Version 9 Template Properties on page 1157](#)
- [Customizing Template ID, Observation Domain ID, and Source ID for Version 9 flow Templates on page 1159](#)
- [Restrictions on page 1159](#)
- [Fields Included in Each Template Type on page 1160](#)
- [MPLS Sampling Behavior on page 1161](#)
- [Verification on page 1162](#)
- [Examples: Configuring Version 9 Flow Templates on page 1162](#)

## Configuring the Traffic to Be Sampled

To specify sampling of IPv4, IPv6, MPLS, or peer AS billing traffic, include the appropriate configuration of the **family** statement at the **[edit forwarding-options sampling]** hierarchy level:

```
[edit forwarding-options]
sampling {
  family (inet | inet6 | mpls);
}
```

You can include **family inet**, **family inet6**, or **family mpls**.



**NOTE:** If you specify sampling for peer AS billing traffic, the **family** statement supports only IPv4 and IPv6 traffic (**inet** or **inet6**). Peer AS billing traffic is enabled only at the global instance hierarchy level and is not available for per Packet Forwarding Engine instances.

After you specify the family of traffic to be sampled, configure the sampling parameters such as the maximum packet length (beyond which the packets are truncated), the maximum packets to be sampled per second (beyond which the packets are dropped), the rate (for example, if you specify 10, every 10th packet is sampled), and run length (which specify the number of packets to be sampled after the trigger; that is if the **rate** is set to 10 and **run-length** to 5, five packets starting the 10th packet are sampled).

```
[edit forwarding-options sampling]
input {
  maximum-packet-length bytes
  max-packets-per-second number;
  rate number;
  run-length number;
}
```

## Configuring the Version 9 Template Properties

To define the version 9 templates, include the following statements at the **[edit services flow-monitoring version9]** hierarchy level:

```
[edit services flow-monitoring version9]
template name {
  options-template-id
  template-id
  source-id
  flow-active-timeout seconds;
  flow-inactive-timeout seconds;
  option-refresh-rate packets packets seconds seconds;
  template-refresh-rate packets packets seconds seconds;
  (ipv4-template | ipv6-template | mpls-ipv4-template | mpls-template |
   peer-as-billing-template) {
    label-position [ positions ];
  }
}
```

The following details apply to the configuration statements:

- You assign each template a unique name by including the **template *name*** statement.
- You then specify each template for the appropriate type of traffic by including the **ipv4-template**, **ipv6-template**, **mpls-ipv4-template**, **mpls-template**, or **peer-as-billing-template**.
- If the template is used for MPLS traffic, you can also specify up to three label positions for the MPLS header label data by including the **label-position** statement; the default values are [1 2 3].
- Within the template definition, you can optionally include values for the **flow-active-timeout** and **flow-inactive-timeout** statements. These statements have specific default and range values when they are used in template definitions; the default is 60 seconds and the range is from 10 through 600 seconds. Values you specify in template definitions override the global timeout values configured at the **[edit forwarding-options sampling family (inet | inet6 | mpls) output flow-server]** hierarchy level.
- You can also include settings for the **option-refresh-rate** and **template-refresh-rate** statements within a template definition. For both of these properties, you can include a timer value (in seconds) or a packet count (in number of packets). For the **seconds** option, the default value is 60 and the range is from 10 through 600. For the **packets** option, the default value is 4800 and the range is from 1 through 480,000.
- To filter IPV6 traffic on a media interface, the following configuration is supported:

```
interfaces interface-name {
  unit 0 {
    family inet6 {
      sampling {
        input;
        output;
      }
    }
  }
}
```

## Customizing Template ID, Observation Domain ID, and Source ID for Version 9 flow Templates

Use of version 9 and IPFIX allows you to define a flow record template suitable for IPv4 traffic, IPv6 traffic, MPLS traffic, a combination of IPv4 and MPLS traffic, or peer AS billing traffic. Templates and the fields included in the template are transmitted to the collector periodically, and the collector need not be aware of the router configuration. Starting with Junos OS Release 14.1, you can specify the unique identifier for the version 9 and IPFIX templates. The identifier of a template is locally unique within a combination of a transport session and an observation domain. Template IDs 0 through 255 are reserved for template sets, options template sets, and other sets for future use. Template IDs of data sets are numbered from 256 through 65535. Typically, this information element or field in the template is used to define the characteristics or properties of other information elements in a template. After a restart of the export process of templates is performed, template IDs can be reassigned. In Junos OS releases earlier than Release 14.1, template IDs and options template IDs were predefined for each address family and could not be modified.

This functionality to configure template ID, options template ID, observation domain ID, and source ID is supported on all routers with MPCs (Trio chip-based FPCs).

The following values were assigned by default for the template IDs of IPFIX templates for the different protocols or address families, until Junos OS Release 13.3:

- IPv4 flow template ID—256
- IPv6 flow template ID—257
- VPLS flow template ID—258
- Options template ID for all address families—512

The corresponding data sets and option data sets contain the value of the template IDs and options template IDs respectively in the set ID field. This method enables the collector to match a data record with a template record.

For more information about specifying the source ID, observation domain ID, template ID, and options template ID for version 9 and IPFIX flows, see [“Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows” on page 1172](#) and [“Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows” on page 1167](#).

## Restrictions

The following restrictions apply to version 9 templates:

- You cannot apply the two different types of flow aggregation configuration (cflowd version 5/8 and flow aggregation version 9) at the same time.
- Flow export based on an **mpls-ipv4** template assumes that the IPv4 header follows the MPLS header. In the case of Layer 2 VPNs, the packet on the provider router (P router) would look like this:

MPLS | Layer 2 Header | IPv4

In this case, **mpls-ipv4** flows are not created on the PIC, because the IPv4 header does not directly follow the MPLS header. Packets are dropped on the PIC and are accounted as parser errors.

- Outbound Routing Engine traffic is not sampled. A firewall filter is applied as output on the egress interface, which samples packets and exports the data. For transit traffic, egress sampling works correctly. For internal traffic, the next hop is installed in the Packet Forwarding Engine but sampled packets are not exported.
- Flows are created on the monitoring PIC only after the route record resynchronization operation is complete, which is 60 seconds after the PIC comes up. Any packets sent to the PIC would be dropped until the synchronization process is complete.



**NOTE:** "Because the forwarding of a packet that arrives with MPLS labels is performed based on the MPLS label and not based on the IP address contained in the packet, the packet is sampled at the output interface with the MPLS label that was popped not being available at the time of sampling. In such a case, depending on the incoming interface (IIF), the VRF index is identified and the route for the sampled packet is determined in the VRF table. Because a specific route is not available in the VRF that is different from the VRF on which the packet is received, the Output Interface Index, Source Mask, and Destination Mask fields are incorrectly populated. This behavior occurs when an IPv4 template is applied as a firewall filter on an egress interface with sample as the action."

---

## Fields Included in Each Template Type

The following fields are common to all template types:

- Input interface
- Output interface
- Number of bytes
- Number of packets
- Flow start time
- Flow end time

The IPv4 template includes the following specific fields:

- IPv4 Source Address
- IPv4 Destination Address
- L4 Source Port
- L4 Destination Port
- IPv4 TOS
- IPv4 Protocol

- ICMP type and code
- TCP Flags
- IPv4 Next Hop Address

The IPv6 template includes the following specific fields:

- IPv6 Source Address and Mask
- IPv6 Destination Address and Mask
- L4 Source Port
- L4 Destination Port
- IPv6 TOS
- IPv6 Protocol
- TCP Flags
- IP Protocol Version
- IPv6 Next Hop Address
- Egress Interface Information
- Source Autonomous System (AS) number
- Destination AS number

The MPLS template includes the following specific fields:

- MPLS Label #1
- MPLS Label #2
- MPLS Label #3
- MPLS EXP Information
- FEC IP Address

The MPLS-IPv4 template includes all the fields found in the IPv4 and MPLS templates.

The peer AS billing template includes the following specific fields:

- IPV4 Class of Service (TOS)
- Ingress Interface
- BGP IPV4 Next Hop Address
- BGP Peer Destination AS Number

## MPLS Sampling Behavior

This section describes the behavior when MPLS sampling is used on egress interfaces in various scenarios (label pop or swap) on provider routers (P routers). For more information

on configuration and background specific to MPLS applications, see the *Junos OS MPLS Applications Library for Routing Devices*.

1. You configure MPLS sampling on an egress interface on the P router and configure an MPLS flow aggregation template. The route action is label *pop* because penultimate hop popping (PHP) is enabled.

Previously, IPv4 packets (only) would have been sent to the PIC for sampling even though you configured MPLS sampling. No flows should be created, with the result that the parser fails.

With the current capability of applying MPLS templates, MPLS flows are created.

2. As in the first case, you configure MPLS sampling on an egress interface on the P router and configure an MPLS flow aggregation template. The route action is label swap and the swapped label is 0 (explicit null).

The resulting behavior is that MPLS packets are sent to the PIC. The flow being sampled corresponds to the label before the swap.

3. You configure a Layer 3 VPN network, in which a customer edge router (CE-1) sends traffic to a provider edge router (PE-A), through the P router, to a similar provider edge router (PE-B) and customer edge router (CE-2) on the remote end.

The resulting behavior is that you cannot sample MPLS packets on the PE-A to P router link.

## Verification

To verify the configuration properties, you can use the **show services accounting aggregation template template-name *name*** operational mode command.

All other **show services accounting** commands also support version 9 templates, except for **show services accounting flow-detail** and **show services accounting aggregation aggregation-type**. For more information about operational mode commands, see the [CLI Explorer](#).

## Examples: Configuring Version 9 Flow Templates

The following is a sample version 9 template configuration:

```
services {
  flow-monitoring {
    version9 {
      template ip-template {
        flow-active-timeout 20;
        flow-inactive-timeout 120;
        ipv4-template;
      }
      template mpls-template-1 {
        mpls-template {
          label-position [1 3 4];
        }
      }
      template mpls-ipv4-template-1 {
```

```

        mpls-ipv4-template {
            label-position [1 5 7];
        }
    }
    template peer-as-billing-template-1 {
        peer-as-billing-template;
    }
}
}
}
}

```

The following is a sample firewall filter configuration for MPLS traffic:

```

firewall {
    family mpls {
        filter mpls_sample {
            term default {
                then {
                    accept;
                    sample;
                }
            }
        }
    }
}

```

The following sample configuration applies the MPLS sampling filter on a networking interface and configures the AS PIC to accept both IPv4 and MPLS traffic:

```

interfaces {
    at-0/1/1 {
        unit 0 {
            family mpls {
                filter {
                    input mpls_sample;
                }
            }
        }
    }
    sp-7/0/0 {
        unit 0 {
            family inet;
            family mpls;
        }
    }
}

```

The following example applies the MPLS version 9 template to the sampling output and sends it to the AS PIC:

```

forwarding-options {
    sampling {
        input {
            family mpls {
                rate 1;
            }
        }
    }
}

```

```

    }
    family mpls {
        output {
            flow-active-timeout 60;
            flow-inactive-timeout 30;
            flow-server 1.2.3.4 {
                port 2055;
                version9 {
                    template mpls-ipv4-template-1;
                }
            }
        }
        interface sp-7/0/0 {
            source-address 1.1.1.1;
        }
    }
}

```

The following is a sample firewall filter configuration for the peer AS billing traffic:

```

firewall {
    family inet {
        filter peer-as-filter {
            term 0 {
                from {
                    destination-class dcu-1;
                    interface ge-2/1/0;
                    forwarding-class class-1;
                }
                then count count_team_0;
            }
            term 1 {
                from {
                    destination-class dcu-2;
                    interface ge-2/1/0;
                    forwarding-class class-1;
                }
                then count count_team_1;
            }
            term 2 {
                from {
                    destination-class dcu-3;
                    interface ge-2/1/0;
                    forwarding-class class-1;
                }
                then count count_team_2;
            }
        }
    }
}

```

The following sample configuration applies the peer AS firewall filter as a filter attribute under the forwarding-options hierarchy for CoS-level data traffic usage information collection:

```

forwarding-options {
  family inet {
    filter output peer-as-filter;
  }
}

```

The following sample configuration applies the peer AS DCU policy options to collect usage statistics for the traffic stream for as-path ingress at a specific input interface with the firewall configuration hierarchy applied as Forwarding Table Filters (FTFs). The configuration functionality with COS capability can be achieved through FTFs for destination-class usage with forwarding-class for specific input interfaces:

```

policy-options {
  policy-statement P1 {
    from {
      protocol bgp;
      neighbor 10.2.25.5; #BGP router configuration;
      as-path AS-1; #AS path configuration;
    }
    then destination-class dcu-1; #Destination class configuration;
  }
  policy-statement P2 {
    from {
      neighbor 1.2.25.5;
      as-path AS-2;
    }
    then destination-class dcu2;
  }
  policy-statement P3 {
    from {
      protocol bgp;
      neighbor 192.2.1.1;
      as-path AS-3;
    }
    then destination-class dcu3;
  }
  as-path AS-1 3131:1111:1123;
  as-path AS-2 100000;
  as-path AS-3 192:29283:2;
}

```

The following example applies the peer-as-billing version 9 template to enable sampling of traffic for billing purposes:

```

forwarding-options {
  sampling {
  }
  input {
    rate 1;
  }
  family inet {
    output {
      flow-server 10.209.15.58 {
        port 300;
        version9 {
          template {

```

```
        peer-as;  
    }  
}  
interface sp-5/2/0 {  
    source-address 2.3.4.5;  
}  
}  
}  
}  
family inet {  
    filter {  
        output peer-as-filter;  
    }  
}
```

**Related  
Documentation**

- *Understanding Flow Aggregation*
- [Enabling Flow Aggregation on page 1151](#)
- [Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd on page 1152](#)
- *Configuring Flow Aggregation to Use IPFIX Flow Templates*
- [Configuring Traffic Sampling on page 1134](#)
- *Example: Configuring Active Flow Monitoring Version 9 for IPv6*

## Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows

Starting with Junos OS Release 14.1, you can define the template ID for version 9 and IPFIX templates for inline flow monitoring. To specify the template ID for version 9 flows, include the **template-id** *id* statement at the **[edit services flow-monitoring version9 template *template-name*]** hierarchy level.

```
[edit services flow-monitoring version9]
template template-name {
  template-id id;
}
```

To specify the template ID for version IPFIX flows, include the **template-id** statement at the **[edit services flow-monitoring version-ipfix template *template-name*]** hierarchy level.

```
[edit services flow-monitoring version-ipfix]
template template-name {
  template-id id;
}
```

To specify the options template ID for version 9 flows, include the **options-template-id** statement at the **[edit services flow-monitoring version9 template *template-name*]** hierarchy level.

```
[edit services flow-monitoring version9]
template template-name {
  options-template-id id;
}
```

To specify the options template ID for version IPFIX flows, include the **options-template-id** statement at the **[edit services flow-monitoring version-ipfix template *template-name*]** hierarchy level. The template ID and options template ID can be a value in the range of 1024 through 65535.

```
[edit services flow-monitoring version-ipfix]
template template-name {
  options-template-id id;
}
```

The template ID and options template ID can be a value in the range of 1024 through 65535. If you do not configure values for the template ID and options template ID, default values are assumed for these IDs, which are different for the various address families. If you configure the same template ID or options template ID value for different address families, such a setting is not processed properly and might cause unexpected behavior. For example, if you configure the same template ID value for both IPv4 and IPv6, the collector validates the export data based on the template ID value that it last receives. In this case, if IPv6 is configured after IPv4, the value is effective for IPv6 and the default value is used for IPv4.

The following are the default values of template IDs for IPFIX flows for the different protocols or address families, until Junos OS Release 13.3:

- IPv4 IPFIX flow template ID—256
- IPv6 IPFIX flow template ID—257
- VPLS IPFIX flow template ID—258
- MPLS IPFIX flow template ID—259

The following are the default values of template IDs for version 9 flows for the different protocols or address families, starting with Junos OS Release 14.1:

- IPv4 version 9 flow template ID—320
- IPv6 version 9 flow template ID—321
- VPLS version 9 flow template ID—322
- MPLS version 9 flow template ID—323

The following are the default values of template IDs for IPFIX flows for the different protocols or address families, until Junos OS Release 13.3:

- IPv4 IPFIX flow options template ID—512
- IPv6 IPFIX flow options template ID—513
- VPLS IPFIX flow options template ID—514
- MPLS IPFIX flow options template ID—515

The following are the default values of template IDs for version 9 flows for the different protocols or address families, starting with Junos OS Release 14.1:

- IPv4 version 9 flow options template ID—576
- IPv6 version 9 flow options template ID—577
- VPLS version 9 flow options template ID—578
- MPLS version 9 flow options template ID—579

[Table 34 on page 1168](#) describes the values of data template and option template IDs for different protocols with default and configured values for IPFIX flows.

**Table 34: Values of Template and Option Template IDs for IPFIX Flows**

Family	Configured Value	Data Template	Option Template
IPv4	None	256	576
IPv4	1024-65535	1024-65535	1024-65535
IPv6	None	257	577
IPv6	1024-65535	1024-65535	1024-65535
VPLS	None	258	578

**Table 34: Values of Template and Option Template IDs for IPFIX Flows** (*continued*)

Family	Configured Value	Data Template	Option Template
VPLS	1024-65535	1024-65535	1024-65535
MPLS	None	259	579
MPLS	1024-65535	1024-65535	1024-65535

[Table 35 on page 1169](#) describes the values of data template and option template IDs for different protocols with default and configured values for version 0 flows.

**Table 35: Values of Template and Option Template IDs for Version 9 Flows**

Family	Configured Value	Data Template	Option Template
IPv4	None	320	576
IPv4	1024-65535	1024-65535	1024-65535
IPv6	None	321	577
IPv6	1024-65535	1024-65535	1024-65535
VPLS	None	322	578
VPLS	1024-65535	1024-65535	1024-65535
MPLS	None	323	579
MPLS	1024-65535	1024-65535	1024-65535

[Table 34 on page 1168](#) describes the values of data template and option template IDs for different protocols with default and configured values for IPFIX flows.

Table 36: Values of Template and Option Template IDs for IPFIX Flows

Configured Value	Protocol Family	FPC Slot	PFE Inst	LU Inst	Observation Domain Id  Conf val rsvd 1proto slot LUInst PFEInst  xxxx xxxx xxxx 1xxx xxxx xxxx xxxx xxxx
None	IPv4 (0)	1	1	0	0000 0000 0000 1000 0000 0001 0000 0001 0x00080101
None	IPv6 (1)	1	1	0	0000 0000 0000 1001 0000 0001 0000 0001 0x00090101
None	VPLS (2)	1	1	0	0000 0000 0000 1010 0000 0001 0000 0001 0x000A0101
None	MPLS (3)	1	1	0	0000 0000 0000 1011 0000 0001 0000 0001 0x000B0101
4	IPv4 (0)	1	1	0	0000 0100 0000 1000 0000 0001 0000 0001 0x04080101
190	IPv4 (0)	1	1	0	1101 1110 0000 1000 0000 0001 0000 0001 0xBE080101
4	IPv4 (0)	2	1	1	0000 0100 0000 1000 0000 0010 0001 0001 0x04080211

Table 36: Values of Template and Option Template IDs for IPFIX Flows (*continued*)

Configured Value	Protocol Family	FPC Slot	PFE Inst	LU Inst	Observation Domain Id Conf val rsvd 1proto slot LUInst PFEInst  xxxx xxxx xxxx 1xxx xxxx xxxx xxxx xxxx
4	IPv6 (1)	1	1	0	0000 0100 0000 1001 0000 0001 0001 0000 0x04090110
190	IPv6 (1)	1	1	0	1101 1110 0000 1001 0000 0001 0001 0000 0xBE090110
4	VPLS (2)	2	2	0	0000 0100 0000 1010 0000 0010 0010 0000 0x040A0220
10	IPv4 (0)	28	2	1	0000 1010 0000 1000 0001 1100 0010 0001 0x0A081C21

**Related Documentation**

- [Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows on page 1172](#)

## Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows

---

For IPFIX flows, an identifier of an Observation Domain is locally unique to an exporting process of the templates. The export process uses the Observation Domain ID to uniquely identify to the collection process in which the flows were metered. We recommend that you configure this ID to be unique for each IPFIX flow. A value of 0 indicates that no specific Observation Domain is identified by this information element. Typically, this attribute is used to limit the scope of other information elements. If the observation domain is not unique, the collector cannot uniquely identify an IPFIX device.

If you configure the same Observation Domain ID for different template types, such as for IPv4 and IPv6, it does not impact flow monitoring because the actual or the base observation domain ID is transmitted in the flow. The actual observation domain ID is derived from the value you configure and also in conjunction with other parameters such as the slot number, lookup chip (LU) instance, Packet Forwarding Engine instance. Such a method of computation of the observation domain ID ensures that this ID is not the same for two IPFIX devices.

Until Junos OS Release 13.3, the observation domain ID is predefined and is set to a fixed value, which is derived from the combination of FPC slot, sampling protocol, PFE Instance and LU Instance fields. This derivation creates a unique observation domain per LU per family. Starting with Junos OS Release 14.1, you can configure the observation domain ID, which causes the first 8 bits of the field to be configured.

The following modifications have been made:

- FPC slots are expanded to 8 bits to enable more slots to be configured in an MX Series Virtual Chassis configuration.
- 8 bits of the configured observation domain ID are used.
- You can configure a value for the observation domain ID in the range of 0 through 255.
- The Protocol field is increased to 3 bits to provide support for additional protocols in inline flow monitoring.
- You can associate the observation domain ID with templates by using the **observation-domain-id *domain-id*** statement at the **[edit services flow- monitoring version-ipfix template *template-name*]** hierarchy level.

For version 9 flows, a 32-bit value that identifies the Exporter Observation Domain is called the source ID. NetFlow collectors use the combination of the source IP address and the source ID field to separate different export streams originating from the same exporter.

To specify the observation domain ID for IPFIX flows, include the **observation-domain-id *domain-id*** statement at the **[edit services flow-monitoring version-ipfix template *template-name*]** hierarchy level.

```
[edit services flow-monitoring version-ipfix]
template template-name {
  observation-domain-id domain-id;
```

```
}

```

To specify the source ID for version 9 flows, include the **source-id** *source-id* statement at the **[edit services flow-monitoring version9 template *template-name*]** hierarchy level.

```
[edit services flow-monitoring version9]
template template-name {
  source-id source-id;
}
```

[Table 37 on page 1173](#) describes observation domain ID values for different combinations of the configured domain ID, protocol family, FPC slot, and the Packet Forwarding Engine and lookup chip instances.

**Table 37: Example of Observation Domain ID**

Configured Value	Protocol Family	FPC Slot	PFE Inst	LU Inst	Observation Domain Id  Conf val rsvd 1proto slot LUInst PFEInst  xxxx xxxx xxxx 1xxx xxxx xxxx xxxx xxxx
None	IPv4 (0)	1	1	0	0000 0000 0000 1000 0000 0001 0000 0001 0x00080101
None	IPv6 (1)	1	1	0	0000 0000 0000 1001 0000 0001 0000 0001 0x00090101
None	VPLS (2)	1	1	0	0000 0000 0000 1010 0000 0001 0000 0001 0x000A0101
None	MPLS (3)	1	1	0	0000 0000 0000 1011 0000 0001 0000 0001 0x000B0101
4	IPv4 (0)	1	1	0	0000 0100 0000 1000 0000 0001 0000 0001 0x04080101

Table 37: Example of Observation Domain ID *(continued)*

Configured Value	Protocol Family	FPC Slot	PFE Inst	LU Inst	Observation Domain Id  Conf val rsvd lproto slot LUInst PFEInst  xxxx xxxx xxxx 1xxx xxxx xxxx xxxx xxxx
190	IPv4 (0)	1	1	0	1101 1110 0000 1000 0000 0001 0000 0001 0xBE080101
4	IPv4 (0)	2	1	1	0000 0100 0000 1000 0000 0010 0001 0001 0x04080211
4	IPv6 (1)	1	1	0	0000 0100 0000 1001 0000 0001 0001 0000 0x04090110
190	IPv6 (1)	1	1	0	1101 1110 0000 1001 0000 0001 0001 0000 0xBE090110
4	VPLS (2)	2	2	0	0000 0100 0000 1010 0000 0010 0010 0000 0x040A0220
10	IPv4 (0)	28	2	1	0000 1010 0000 1000 0001 1100 0010 0001 0x0A081C21

**Related Documentation**

- [Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 1167](#)

## Sampling Instance Configuration

You can configure active sampling by defining a sampling instance that specifies a name for the sampling parameters and bind the instance name to an FPC, MPC, or DPC. This configuration enables you to define multiple named sampling parameter sets associated with multiple destinations and protocol families per sampling destination. With the cflowd version 5 and version 8 and flow aggregation version 9, you can use templates to organize the data gathered from sampling.

To implement this feature, you include the **instance** statement at the **[edit forwarding-options sampling]** hierarchy level.

The following considerations apply to the sampling instance configuration:

- This configuration is supported on the IP version 4 (**inet**), IP version 6 (**ipv6**), and MPLS protocol families.
- You can configure the router to perform sampling in either of two locations:
  - On the Routing Engine, using the sampled process. To select this method, use a filter (input or output) with a matching term that contains the **then** sample statement.
  - On the Monitoring Services, Adaptive Services, or Multiservices PIC. Specify the interface name at the **[forwarding-options sampling instance *instance-name* family inet output interface]** hierarchy level. You can configure the same or different services PICs in a set of sampling instances.
- You can configure the **rate** and **run-length** options at the **[edit forwarding-options sampling input]** hierarchy level to apply common values for all families on a global basis. Alternatively, you can configure these options at the **[edit forwarding-options sampling instance *instance-name* input]** hierarchy level to apply specific values for each instance or at the **[edit forwarding-options sampling instance *instance-name* family *family-name* input]** hierarchy level to apply specific values for each protocol family you configure.
- For MX Series devices with Modular Port Concentrators (MPCs), port-mirrored or sampled packets can be truncated (or clipped) to any length in the range of 1 through 255 bytes. Only the values 1 to 255 are valid for packet truncation on these devices. For other devices, the range is from 0 through 9216. A maximum-packet-length value of zero (0) represents that truncation is disabled, and the entire packet is mirrored or sampled.



**NOTE:** The **run-length** and **maximum-packet-length** configuration statements are not supported on MX80 routers.

To associate the defined instance with a particular FPC, MPC, or DPC, you include the **sampling-instance** statement at the **[edit chassis fpc *number*]** hierarchy level, as in the following example:

```
chassis {
```

```
fpc 2 {  
    sampling-instance samp1;  
}
```

To associate a sampling instance with an FPC in the MX Series Virtual Chassis master or backup router, use the **sampling-instance *instance-name*** statement at the **[edit chassis member *member-number* fpc slot *slot-number*]** hierarchy level, where *member-number* is 0 (for the master router) or 1 (for the backup router), and *slot-number* is a number in the range 0 through 11.

#### Related Documentation

- *Traffic Sampling, Forwarding, and Monitoring Overview*
- *Flow Monitoring Feature Guide for Routing Devices*
- *More Information About Passive and Active Flow Monitoring*
- *Configuring Active Flow Monitoring*
- *Configuring Flow Aggregation (cflowd)*
- [Configuring Traffic Sampling on page 1134](#)
- *Example: Sampling Instance Configuration*
- *[edit forwarding-options sampling] Hierarchy Level*
- *Inline Flow Monitoring for Virtual Chassis Overview*

---

## Configuring Inline Sampling

On MX Series routers and EX 9200 switches, you can configure active sampling to be performed on an inline data path without the need for a services Dense Port Concentrator (DPC). To do this, you define a sampling instance with specific properties. One Flexible PIC Concentrator (FPC) can support only one instance; for each instance, either services PIC-based sampling or inline sampling is supported per family. As a result, a particular instance can define PIC-based sampling for one family and inline sampling for a different family. Both IPv4 and IPv6 are supported for inline sampling.

Inline sampling supports version 9 and IPFIX flow collection templates. Support for version 9 template was introduced in Junos OS Release 13.2, and is limited to IPv4 flows. IPFIX template is supported for IPv4, IPv6, and VPLS flows. IPFIX template uses UDP as the transport protocol, whereas version 9 is transport protocol-independent.

The following limitations exist for inline sampling:

- Flow records and templates cannot be exported if the flow collector is reachable through any management interface.
- The flow collector should be reachable through the default routing table (inet.0 or inet6.0). If the flow collector is reachable via a non-default VPN routing and forwarding table (VRF), flow records and templates cannot be exported.



**NOTE:** Starting with Junos OS Release 13.3, you can configure the flow collector to be reachable through non-default VRF instances apart from being reachable over the default VRF instance. Flow records and templates can be exported even with non-default VRF instances.

- If the destination of the sampled flow is reachable through multiple paths, the IP\_NEXT\_HOP (Element ID 15) and OUTPUT\_SNMP (Element ID 14) in the IPv4 flow record would be set to the Gateway Address and SNMP Index of the first path seen in the forwarding table.
- If the destination of the sampled flow is reachable through multiple paths, the IP\_NEXT\_HOP (Element ID 15) and OUTPUT\_SNMP (Element ID 14) in the IPv6 flow records would be set to 0.
- The user-defined sampling instance gets precedence over the global instance. When a user-defined sampling instance is attached to the FPC, the global instance is removed from the FPC and the user-defined sampling instance is applied to the FPC.
- The Incoming Interface (IIF) and Outgoing Interface (OIF) should be part of the same VRF. If OIF is in a different VRF, DST\_MASK (Element ID 13), DST\_AS (Element ID 17), IP\_NEXT\_HOP (Element ID 15), and OUTPUT\_SNMP (Element ID 14) would be set to 0 in the flow records.
- Each Lookup Chip (LU) maintains and exports flows independent of other LUs. Traffic received on a media interface is distributed across all LUs in a multi-LU platform. It is likely that a single flow will be processed by multiple LUs. Therefore, each LU creates a unique flow and exports it to the flow collector. This can cause duplicate flows records to be seen on the flow collector. The flow collector should aggregate PKTS\_COUNT and BYTES\_COUNT for duplicate flow records to derive a single flow record.

Before you configure inline sampling, you should ensure that you have adequately-sized hash tables for IPv4 and IPv6 flow sampling. These tables can use one to fifteen 256k areas, and each table is assigned a default value of one such area. When anticipated traffic volume requires larger tables, allocate larger tables.



**NOTE:** For Junos OS releases earlier than Release 12.1, the following points are applicable for supporting backward compatibility when you configure the IPv4 and IPv6 flow table sizes for inline sampling:

- If you do not configure the `flow-table-size` statement at the `[edit chassis fpc slot-number inline-services]` hierarchy level, fifteen 256K entries are allocated by default for the IPv4 flow table and one 1K entry is allocated by default for the IPv6 flow table on the Packet Forwarding Engine.
- If you configure the `ipv4-flow-table-size size` statement at the `[edit chassis fpc slot-number inline-services flow-table-size]` hierarchy level and if you do not configure the `ipv6-flow-table-size size` statement at the `[edit chassis fpc slot-number inline-services flow-table-size]` hierarchy level, the number of units of 256K entries that you configure for the IPv4 flow table is allocated. For the IPv6 flow table, a default size of one 1K entry is allocated on the Packet Forwarding Engine.
- If you do not configure the `ipv4-flow-table-size size` statement at the `[edit chassis fpc slot-number inline-services flow-table-size]` hierarchy level and if you configure the `ipv6-flow-table-size size` statement at the `[edit chassis fpc slot-number inline-services flow-table-size]` hierarchy level, the number of units of 256K entries that you configure for the IPv6 flow table is allocated. For the IPv4 flow table, a default size of one 1K entry is allocated on the Packet Forwarding Engine.
- If you configure the sizes of both the IPv4 and IPv6 flow tables, the flow tables are created on the Packet Forwarding Engine based on the size that you specified.

---

To allocate IPv4 and IPv6 flow hash tables:

1. Go to the `flow-table-size` hierarchy level for inline services on the FPC that processes the monitored flows.

```
[edit]
user@host# edit chassis fpc 0 inline-services flow-table-size
```

2. Specify the required sizes for the sampling hash tables.

```
[edit chassis fpc 0 inline-services flow-table-size]
user@host# set ipv4-flow-table-size 5
user@host# set ipv6-flow-table-size 5
```



**NOTE:** When you set the flow hash table sizes, remember:

- Any change in the configured size of flow hash table sizes initiates an automatic reboot of the FPC.
  - The total number of units used for both IPv4 and IPv6 cannot exceed 15.
-

The configuration for inline sampling on MX80 routers is slightly different.

To configure inline sampling on all other MX Series routers and EX Series switches:

1. Enable inline sampling and specify the source address for the traffic.

```
[edit forwarding-options sampling instance instance-name family inet output]
user@host# set inline-jflow source address address
```

2. Specify the IP\_FIX output format.

```
[edit forwarding-options sampling instance instance-name family inet output flow-server
address]
user@host# set version-ipfix template ipv4
```

3. Specify the output properties.

```
[edit services flow-monitoring]
user@host# set version-ipfix
```

The output format properties are common to other output formats and are described in “*Configuring Flow Aggregation to Use IPFIX Flow Templates*”.

The following is an example of the sampling configuration for an instance that supports inline sampling on **family inet** and PIC-based sampling on **family inet6**:

```
[edit forwarding-options]
sampling {
  instance {
    sample-ins1 {
      input {
        rate 1;
      }
      family inet {
        output {
          flow-server 2.2.2.2 {
            port 2055;
            version-ipfix {
              template {
                ipv4;
              }
            }
          }
        }
        inline-jflow {
          source-address 10.11.12.13;
        }
      }
    }
  }
  family inet6 {
    output {
      flow-server 2.2.2.2 {
        port 2055;
        version-ipfix {
          template {
            ipv6;
          }
        }
      }
    }
  }
}
```

```

        interface sp-0/1/0 {
            source-address 10.11.12.13;
        }
    }
}

```

The following example shows the output format configuration:

```

services {
    flow-monitoring {
        version-ipfix {
            template ipv4 {
                flow-active-timeout 60;
                flow-inactive-timeout 60;
                ipv4-template;
                template-refresh-rate {
                    packets 1000;
                    seconds 10;
                }
                option-refresh-rate {
                    packets 1000;
                    seconds 10;
                }
            }
        }
    }
}

```

The following considerations apply to the inline flow-monitoring instance configuration:

- Sampling run-length and clip-size are not supported.
- For inline configurations, each family can support only one collector.



**NOTE:** Inline sampling instances can handle only up to 65536 AS paths. If the total number of AS paths exceed the maximum limit, the AS paths that have AS index greater than 65536 are discarded and counted as error. Flow records associated with such AS paths show the AS value as `0xFFFFFFFF`. However, this limitation does not impact normal forwarding operations.



**NOTE:** On routers with Multiservices PICs or Multiservices DPCs, all fragments of a fragmented IPv4 packet other than the first fragment of the packet are processed accurately by the flow monitoring application running on MS-PIC or MS-DPC. The flow monitoring mechanism handles such fragments accurately by setting the layer 4 related fields in the associated flows to zero.

Related  
Documentation

- [Configuring Inline Sampling on MX80 Routers on page 1181](#)

- [inline-jflow on page 1243](#)

## Configuring Inline Sampling on MX80 Routers

To configure inline sampling on MX80 routers:

1. Associate a sampling instance with the Forwarding Engine Processor.

```
[edit]
user@host# set chassis tfeb slot number sampling-instance sampling-instance
```

The Forwarding Engine Processor slot is always 0 because MX80 routers have only one Packet Forwarding Engine. In this configuration, the sampling instance is **sample-ins1**.

```
[edit]
user@host# set chassis tfeb slot 0 sampling-instance sample-ins1
```



**NOTE:** MX80 routers support only one sampling instance.

2. Under forwarding-options, configure a sampling instance for the flow server and inline jflow instances (these will be configured in the following steps):

```
[edit forwarding-options sampling]
user@host# edit instance inline_sample
```

3. Configure the rate at the **[edit forwarding-options sampling instance instance-name input]** hierarchy level to apply specific values for the sampling instance **sample-ins1**.

```
[edit forwarding-options sampling instance sample-ins1 input]
user@host# set rate number
```

In this configuration, the rate is 1000.

```
[edit forwarding-options sampling instance sample-ins1 input]
user@host# set rate 1000
```

4. Navigate to the output hierarchy and from there, enable a flow server and then specify the output address and port:

```
[edit] forwarding-options sampling instance inline_sample family inet output]
user@host# edit flow-server address
```

```
[edit forwarding-options sampling instance inline_sample family inet output flow-server
<address>]
user@host# set port number
```

5. Return to the output hierarchy and specify the source address for inline jflow:

```
[edit forwarding-options sampling instance sample-ins1 family inet output]
user@host# set inline-jflow source-address address
```

In this configuration, the source address is 10.11.12.13.

```
[edit forwarding-options sampling instance sample-ins1 family inet output]
user@host# set inline-jflow source-address 10.11.12.13
```

6. Specify the output properties.

```
[edit services flow-monitoring]
user@host# set version-ipfix
```

The output format properties are common to other output formats and are described in *"Configuring Flow Aggregation to Use IPFIX Flow Templates"*.

The following is an example of the sampling configuration for an instance that supports inline sampling on MX80 routers:

```
[edit forwarding-options]
user@host# show
sampling {
  instance {
    sample-ins1 {
      input {
        rate 1000;
      }
      family inet {
        flow-server 133.13.13.122 {
          port 1333;
          inline-jflow {
            source-address 10.11.12.13;
          }
        }
      }
    }
  }
}
```



**NOTE:** You need not configure a Flexible PIC Concentrator (FPC) slot because MX80 routers have only one Packet Forwarding Engine.

---

The following considerations apply to the inline flow-monitoring instance configuration:

- This configuration does not support MPLS-IPv6.
- Clip-size is not supported.

**Related  
Documentation**

- [Configuring Flow Aggregation to Use IPFIX Flow Templates](#)
- [Configuring Inline Sampling on page 1176](#)
- [inline-jflow on page 1243](#)

---

## Directing Replicated Flows to Multiple Flow Servers

You can configure replication of the sampled flow records for use by multiple flow servers. You can use either sampling based on the Routing Engine, using cflowd version 5 or

version 8, or sampling based on the services PIC, using flow aggregation version 9, as described in the following sections:

- [Directing Replicated Routing Engine–Based Sampling Flows to Multiple Servers on page 1183](#)
- [Directing Replicated Version 9 Flow Aggregates to Multiple Servers on page 1184](#)

## Directing Replicated Routing Engine–Based Sampling Flows to Multiple Servers

Routing Engine–based sampling supports up to eight flow servers for both cflowd version 5 and version 8 configurations. The total number of servers is limited to eight regardless of how many are configured for cflowd v5 or v8.

When you configure cflowd-based sampling, the export packets are replicated to all flow servers configured to receive them. If two servers are configured to receive v5 records, both the servers will receive records for a specified flow.



**NOTE:** With Routing Engine–based sampling, if multiple flow servers are configured with version 8 export format, all of them must use the same aggregation type. For example, all servers receiving version 8 export could be configured for source-destination aggregation type.

The following configuration example allows replication of export packets to two flow servers.

```
forwarding-options {
  sampling {
    instance inst1 {
      input {
        rate 1;
      }
      family inet;
      output {
        flow-server 10.10.3.2 {
          port 2055;
          version 5;
          source-address 192.168.164.119;
        }
        flow-server 172.17.20.62 {
          port 2055;
          version 5;
          source-address 192.168.164.119;
        }
      }
    }
  }
}
```

## Directing Replicated Version 9 Flow Aggregates to Multiple Servers

The export packets generated for a template are replicated to all the flow servers that are configured to receive information for that template. The maximum number of servers supported is eight.

This also implies that periodic updates required by version 9 (RFC 3954) are sent to each configured collector. The following updates are sent periodically as part of this requirement:

- Options data
- Template definition

The refresh period for options data and template definition is configured on a per-template basis at the **[edit services flow-monitoring]** hierarchy level.

The following configuration example allows replication of version 9 export packets to two flow servers.

```
forwarding-options {
  sampling {
    instance inst1 {
      input {
        rate 1;
      }
      family inet;
      output {
        flow-server 10.10.3.2 {
          port 2055;
          version9 {
            template {
              ipv4;
            }
          }
        }
        flow-server 172.17.20.62 {
          port 2055;
          version9 {
            template {
              ipv4;
            }
          }
        }
      }
      flow-inactive-timeout 30;
      flow-active-timeout 60;
      interface sp-4/0/0 {
        source-address 10.10.3.4;
      }
    }
  }
}
```

**Related Documentation**

- [Active Flow Monitoring Overview on page 1125](#)
- [Configuring Flow Monitoring on page 1144](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 1210](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 1148](#)

## Logging cflowd Flows Before Export

To collect the cflowd flows in a log file before they are exported, include the **local-dump** statement at the **[edit forwarding-options sampling output flow-server *hostname*]** hierarchy level:

```
[edit forwarding-options sampling output flow-server hostname]
local-dump;
```

By default, the flows are collected in **/var/log/sampled**; to change the filename, include the **filename** statement at the **[edit forwarding-options sampling traceoptions]** hierarchy level. For more information about changing the filename, see [“Configuring Traffic Sampling Output” on page 1138](#).



**NOTE:** Because the **local-dump** statement adds extra overhead, you should use it only while debugging cflowd problems, not during normal operation.

The following is an example of the flow information. The AS number exported is the origin AS number. All flows that belong under a cflowd header are dumped, followed by the header itself:

```
Jun 27 18:35:43 v5 flow entry
Jun 27 18:35:43   Src addr: 192.53.127.1
Jun 27 18:35:43   Dst addr: 192.6.255.15
Jun 27 18:35:43   Nhop addr: 192.6.255.240
Jun 27 18:35:43   Input interface: 5
Jun 27 18:35:43   Output interface: 3
Jun 27 18:35:43   Pkts in flow: 15
Jun 27 18:35:43   Bytes in flow: 600
Jun 27 18:35:43   Start time of flow: 7230
Jun 27 18:35:43   End time of flow: 7271
Jun 27 18:35:43   Src port: 26629
Jun 27 18:35:43   Dst port: 179
Jun 27 18:35:43   TCP flags: 0x10
Jun 27 18:35:43   IP proto num: 6
Jun 27 18:35:43   TOS: 0xc0
Jun 27 18:35:43   Src AS: 7018
Jun 27 18:35:43   Dst AS: 11111
Jun 27 18:35:43   Src netmask len: 16
Jun 27 18:35:43   Dst netmask len: 0
```

[... 41 more version 5 flow entries; then the following header:]

```
Jun 27 18:35:43 cflowd header:
Jun 27 18:35:43   Num-records: 42
Jun 27 18:35:43   Version: 5
Jun 27 18:35:43   low seq num: 118
```

Jun 27 18:35:43 Engine id: 0  
Jun 27 18:35:43 Engine type: 3

**Related  
Documentation**

- [Active Flow Monitoring Overview on page 1125](#)
- [Configuring Flow Monitoring on page 1144](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 1182](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 1210](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 1148](#)

---

## Configuring Port Mirroring

To prepare traffic for port mirroring, include the **filter** statement at the **[edit firewall family inet]** hierarchy level:

```
filter filter-name;
```

This filter at the **[edit firewall family (inet | inet6)]** hierarchy level selects traffic to be port-mirrored:

```
filter filter-name {  
  term term-name {  
    then {  
      port-mirror;  
      accept;  
    }  
  }  
}
```

To configure port mirroring on a logical interface, configure the following statements at the **[edit forwarding-options port-mirroring]** hierarchy level:

```
[edit forwarding-options port-mirroring]  
input {  
  maximum-packet-length bytes  
  rate rate;  
  run-length number;  
}  
family (inet|inet6) {  
  output {  
    interface interface-name {  
      next-hop address;  
    }  
  }  
  no-filter-check;  
}
```



**NOTE:** The input statement is deprecated at the **[edit forwarding-options port-mirroring family (inet | inet6)]** hierarchy level and is maintained only for backward compatibility. You must include the input statement at the **[edit forwarding-options port-mirroring]** hierarchy level.

---

Specify the port-mirroring destination by including the **next-hop** statement at the **[edit forwarding-options port-mirroring output interface *interface-name*]** hierarchy level:

```
next-hop address;
```



**NOTE:** For IPv4 port mirroring to reach a next-hop destination, you must manually include a static Address Resolution Protocol (ARP) entry in the router configuration.

The **no-filter-check** statement is required when you send port-mirrored traffic to a Tunnel PIC that has a filter applied to it. en

The interface used to send the packets to the analyzer is the output interface configured above at the **[edit forwarding-options port-mirroring family (inet | inet6) output]** hierarchy level. You can use any physical interface type, including generic routing encapsulation (GRE) tunnel interfaces. The next-hop address specifies the destination address; this statement is mandatory for non point-to-point interfaces, such as Ethernet interfaces.

To configure the sampling rate or duration, include the **rate** or **run-length** statement at the **[edit forwarding-options port-mirroring input]** hierarchy level.

You can trace port-mirroring operations the same way you trace sampling operations. For more information, see [“Tracing Traffic Sampling Operations” on page 1140](#).

For more information about port mirroring, see the following sections:

- [Configuring Tunnels on page 1187](#)
- [Port Mirroring with Next-Hop Groups on page 1188](#)
- [Configuring Inline Port Mirroring on page 1189](#)
- [Filter-Based Forwarding with Multiple Monitoring Interfaces on page 1190](#)
- [Restrictions on page 1190](#)
- [Configuring Port Mirroring on Services Interfaces on page 1191](#)
- [Examples: Configuring Port Mirroring on page 1192](#)

## Configuring Tunnels

In typical applications, you send the sampled packets to an analyzer or a workstation for analysis, rather than another router. If you must send this traffic over a network, you should use tunnels. For more information about tunnel interfaces, see *Tunnel Properties*.

If your router is equipped with a Tunnel PIC, you can forward duplicate packets to multiple interfaces by configuring a next-hop group. To configure a next-hop group, include the **next-hop-group** statement at the **[edit forwarding-options]** hierarchy level:

```
[edit forwarding-options]
next-hop-group group-names {
  interface interface-name {
    next-hop address;
  }
}
```

```
}
```

The **interface** statement specifies the interface that sends out sampled information. The **next-hop** statement specifies the next-hop addresses to which to send the sampled information.

Next-hop groups have the following properties:

- Next-hop groups are supported for inet, inet6 and bridge family.
- Next-hop groups are supported on M Series and MX Series routers.
- Next-hop groups support up to 16 next-hop addresses.
- Up to 30 next-hop groups are supported.
- Each next-hop group is expected to have at least two next-hop addresses.

## Port Mirroring with Next-Hop Groups

You can configure next-hop groups for MX, TX, and T Series routers using either IP addresses or Layer 2 addresses for the next hops. Use the **group-type [ inet | layer-2 ]** statement at the **[edit forwarding-options next-hop-group next-hop-group-name]** hierarchy level to establish the next-hop groups. You can reference more than one port mirroring instance in a filter on MX Series routers. Use the **port-mirror-instance instance-name** statement at the **[edit firewall family family-name filter filter-name term term-name]** to refer to one of several port mirroring instances. For more information about this configuration, see the *Layer 2 Port Mirroring Feature Guide for Routing Devices*.



**NOTE:** On the Trio chipset for MX series routers, port mirroring instances can only be bound to the FPC level and not up to the PIC level. For MX series routers with a DPC card, both levels are supported.

On MX, TX, and T Series routers only, you can configure port mirroring using next-hop groups, also known as *multipacket port mirroring*, without the presence of a Tunnel PIC. To configure this functionality, include the **next-hop-group** statement at the **[edit forwarding-options port-mirror family inet output]** or **[edit forwarding-options port-mirror instance instance-name family inet output]** hierarchy level:

```
[edit forwarding-options]
port-mirror {
  family inet {
    output {
      next-hop-group group-name;
    }
  }
}
```

or

```
[edit forwarding-options]
port-mirror {
  instance instance-name {
```

```

family (inet | vpls) {
    output {
        next-hop-group group-name;
    }
}

```

You define the next-hop group by including the **next-hop-group** statement at the **[edit forwarding-options]** hierarchy level. For an example, see [“Examples: Configuring Port Mirroring” on page 1192](#). This configuration is supported only with IPv4 addresses.

You can disable this configuration by including a **disable** or **disable-all-instances** statement at the **[edit forwarding-options port-mirror]** hierarchy level or by including a **disable** statement at the **[edit forwarding-options port-mirror instance *instance-name*]** hierarchy level. You can display the settings and network status by issuing the **show forwarding-options next-hop-group** and **show forwarding-options port-mirroring** operational commands.



**NOTE:** If you try to bind any derived instance to the FPC, a commit error will occur.

## Configuring Inline Port Mirroring

Inline port mirroring provides you with the ability to specify instances that are not bound to the flexible PIC concentrator (FPC) in the firewall filter's **then port-mirror-instance** action. This way, you are not limited to only two port-mirror instances per FPC. Inline port mirroring decouples the port-mirror destination from the input parameters like **rate**. While the input parameters are programmed in the switch interface board, the next-hop destination of the mirrored packet is available in the packet itself. Inline port mirroring is supported only on Trio-based modular port concentrators (MPCs).

Using inline port mirroring, a port-mirror instance will have an option to inherit input parameters from another instance that specifies it, as shown in the following CLI configuration example:

```

instance pm2 {
    + input-parameters-instance pm1;
    family inet {
        output {
            interface ge-1/2/3.0 {
                next-hop 50.0.0.3;
            }
        }
    }
}

```

Multiple levels of inheritance are not allowed. One instance can be referred by multiple instances. An instance can refer to another instance that is defined before it. Forward references are not allowed and an instance cannot refer to itself, doing so will cause an error during configuration parsing.

The user can specify an instance that is not bound to the FPC in the firewall filter. The specified filter should inherit one of the two instances that have been bound to the FPC. If it does not, the packet is not marked for port-mirroring. If it does, then the packet will be sampled using the input parameters specified by the referred instance but the copy will be sent to the its own destination.

## Filter-Based Forwarding with Multiple Monitoring Interfaces

If port-mirrored packets are to be distributed to multiple monitoring or collection interfaces based on patterns in packet headers, it is helpful to configure a filter-based forwarding (FBF) filter on the port-mirroring egress interface.

When an FBF filter is installed as an output filter, a packet that is forwarded to the filter has already undergone at least one route lookup. After the packet is classified at the egress interface by the FBF filter, it is redirected to another routing table for additional route lookup. Obviously, the route lookup in the latter routing table (designated by an FBF routing instance) must result in a different next hop from those from the previous tables the packet has passed through, to avoid packet looping inside the Packet Forwarding Engine.

For more information about FBF configuration, see the *Junos OS Routing Protocols Library for Routing Devices*. For an example of FBF applied to an output interface, see [“Examples: Configuring Port Mirroring” on page 1192](#).

## Restrictions

The following restrictions apply to port-mirroring configurations:

- The interface you configure for port mirroring should not participate in any kind of routing activity.
- The destination address you specify should not have a route to the ultimate traffic destination. For example, if the sampled IPv4 packets have a destination address of **10.68.9.10** and the port-mirrored traffic is sent to **10.68.20.15** for analysis, the device associated with the latter address should not know a route to **10.68.9.10**. Also, it should not send the sampled packets back to the source address.
- IPv4 and IPv6 traffic is supported. For IPv6 port mirroring, you must configure the next-hop router with an IPv6 neighbor before mirroring the traffic, similar to an ARP request for IPv4 traffic. All the restrictions applied to IPv4 configurations should also apply to IPv6.
- On M120 and M320 routers, multiple next-hop mirroring is not supported.
- Because M320 routers do not support multiple bindings of port-mirror instances per FPC, the **port-mirror-instance** action is not supported in firewall filters for these routers.
- On M Series routers other than the M120 and M320 routers, only one family protocol (either IPv4 or IPv6) is supported at a time.
- Port mirroring supports up to 16 next hops, but there is no next-hop group support for **inet6**.
- Only transit data is supported.

- You can configure multiple port-mirroring interfaces per router.
- On routers containing an Internet Processor II application-specific integrated circuit (ASIC), you must include a firewall filter with both the **accept** action and the **port-mirror** action modifier on the inbound interface. Do not include the **discard** action, or port mirroring will not work.
- If the port-mirroring interface is a non-point-to-point interface, you must include an IP address under the **port-mirroring** statement to identify the other end of the link. This IP address must be reachable for you to see the sampled traffic. If the port-mirroring interface is an Ethernet interface, the router should have an Address Resolution Protocol (ARP) entry for it. The following sample configuration sets up a static ARP entry.
- You do not need to configure firewall filters on both inbound and outbound interfaces, but at least one is necessary on the inbound interface to provide the copies of the packets to send to an analyzer.
- Inline port mirroring is supported only on Trio-based MPCs.
- Configuration for both port mirroring and traffic sampling are handled by the same daemon, so in order to view a trace log file for port mirroring, you must configure the **traceoptions** option under traffic sampling.

## Configuring Port Mirroring on Services Interfaces

A special situation arises when you configure unit **0** of a services interface (AS or Multiservices PIC) to be the port-mirroring logical interface, as in the following example:

```
[edit forwarding-options]
port-mirroring {
  input {
    rate 1;
  }
  family inet {
    output {
      interface sp-1/0/0.0;
    }
  }
}
```

Since any traffic directed to unit **0** on a services interface is targeted for monitoring (cflowd packets are generated for it), the sample port-mirroring configuration indicates that the customer would like to have cflowd records generated for the port-mirrored traffic.

However, generation of cflowd records requires the following additional configuration; if it is missing, the port-mirrored traffic is simply dropped by the services interface without generating any cflowd packets.

```
[edit forwarding-options]
sampling {
  instance instance1 { # named instances of sampling parameters
    input {
      rate 1;
    }
  }
}
```

```

family inet {
  output {
    flow-server 172.16.28.65 {
      port 1230;
    }
    interface sp-1/0/0 { # If the port-mirrored traffic requires monitoring, this
                        # interface must be same as that specified in the
                        # port-mirroring configuration.
      source-address 3.1.2.3;
    }
  }
}

```



**NOTE:** Another way to configure `sp-1/0/0` to generate `cflowd` records is to use only the sampling configuration, but include a firewall filter `sample` action instead of a `port-mirror` action.

## Examples: Configuring Port Mirroring

The following example sends port-mirrored traffic to multiple `cflowd` servers or packet analyzers:

```

[edit interfaces]
ge-1/0/0 { # This is the input interface where packets enter the router.
  unit 0 {
    family inet {
      filter {
        input mirror_pkts; # Here is where you apply the first filter.
      }
      address 10.11.0.1/24;
    }
  }
}
ge-1/1/0 { # This is an exit interface for HTTP packets.
  unit 0 {
    family inet {
      address 10.12.0.1/24;
    }
  }
}
ge-1/2/0 { # This is an exit interface for HTTP packets.
  unit 0 {
    family inet {
      address 10.13.0.1/24;
    }
  }
}
so-0/3/0 { # This is an exit interface for FTP packets.
  unit 0 {
    family inet {
      address 10.1.1.1/30;
    }
  }
}

```

```

    }
  }
}
so-4/3/0 { # This is an exit interface for FTP packets.
  unit 0 {
    family inet {
      address 10.2.2.2/30;
    }
  }
}
so-7/0/0 { # This is an exit interface for all remaining packets.
  unit 0 {
    family inet {
      address 10.5.5.5/30;
    }
  }
}
so-7/0/1 { # This is an exit interface for all remaining packets.
  unit 0 {
    family inet {
      address 10.6.6.6/30;
    }
  }
}
vt-3/3/0 { # The tunnel interface is where you send the port mirrored traffic.
  unit 0 {
    family inet;
  }
  unit 1 {
    family inet {
      filter {
        input collect_pkts; # This is where you apply the second firewall filter.
      }
    }
  }
}
[edit forwarding-options]
port-mirroring { # This is required when you configure next-hop groups.
  input {
    rate 1; # This rate port mirrors one packet for every one received (1:1 = all
    # packets).
  }
  family inet {
    output { # This sends traffic to a tunnel interface to prepare for multiport mirroring.
      interface vt-3/3/0.1;
      no-filter-check;
    }
  }
}
next-hop-group ftp-traffic { # Point-to-point interfaces require you to specify the interface
  # name only.
  interface so-4/3/0.0;
  interface so-0/3/0.0;
}
next-hop-group http-traffic { # You need to configure a next hop for multipoint interfaces
  # (Ethernet).

```

```

interface ge-1/1/0.0 {
  next-hop 10.12.0.2;
}
interface ge-1/2/0.0 {
  next-hop 10.13.0.2;
}
}
next-hop-group default-collect {
  interface so-7/0/0.0;
  interface so-7/0/1.0;
}
[edit firewall]
family inet {
  filter mirror_pkts { # Apply this filter to the input interface.
    term catch_all {
      then {
        count input_mirror_pkts;
        port-mirror; # This action sends traffic to be copied and port mirrored.
        accept;
      }
    }
  }
  filter collect_pkts { # Apply this filter to the tunnel interface.
    term ftp-term { # This term sends FTP traffic to an FTP next-hop group.
      from {
        protocol ftp;
      }
      then next-hop-group ftp-traffic;
    }
    term http-term { # This term sends HTTP traffic to an HTTP next-hop group.
      from {
        protocol http;
      }
      then next-hop-group http-traffic;
    }
    term default { # This term sends all remaining traffic to a final next-hop group.
      then next-hop-group default-collectors;
    }
  }
}
}

```

The following example demonstrates configuration of filter-based forwarding at the output interface. In this example, the packet flow follows this path:

1. A packet arrives at interface **fe-1/2/0.0** with source and destination addresses **10.50.200.1** and **10.50.100.1**, respectively.
2. The route lookup in routing table **inet.0** points to the egress interface **so-0/0/3.0**.
3. The output filter installed at **so-0/0/3.0** redirects the packet to routing table **fbf.inet.0**.
4. The packet matches the entry **10.50.100.0/25**, and finally leaves the router from interface **so-2/0/0.0**.

```

[edit interfaces]
so-0/0/3 {
  unit 0 {

```

```
family inet {
  filter {
    output fbf;
  }
  address 10.50.10.2/25;
}
}
fe-1/2/0 {
  unit 0 {
    family inet {
      address 10.50.50.2/25;
    }
  }
}
so-2/0/0 {
  unit 0 {
    family inet {
      address 10.50.20.2/25;
    }
  }
}
[edit firewall]
filter fbf {
  term 0 {
    from {
      source-address {
        10.50.200.0/25;
      }
    }
    then routing-instance fbf;
  }
  term d {
    then count d;
  }
}
[edit routing-instances]
fbf {
  instance-type forwarding;
  routing-options {
    static {
      route 10.50.100.0/25 next-hop so-2/0/0.0;
    }
  }
}
[edit routing-options]
interface-routes {
  rib-group inet fbf-group;
}
static {
  route 10.50.100.0/25 next-hop 10.50.10.1;
}
rib-groups {
  fbf-group {
    import-rib [ inet.0 fbf.inet.0 ];
  }
}
```

```
}
```

The following example shows configuration of port mirroring using next-hops groups or multipacket port mirroring:

```
forwarding-options {
  next-hop-group inet_nhg {
    group-type inet;
    interface ge-2/0/2.101 {
      next-hop 10.2.0.2;
    }
    interface ge-2/2/8.2 {
      next-hop 10.8.0.2;
    }
  }
  next-hop-group vpls_nhg {
    group-type layer-2;
    interface ge-2/0/1.100;
    interface ge-2/2/9.0;
    inactive: next-hop-subgroup vpls_subg {
      interface ge-2/0/1.101;
      interface ge-2/2/9.1;
    }
  }
  next-hop-group vpls_nhg_2 {
    group-type layer-2;
    interface ge-2/2/1.100;
    interface ge-2/3/9.0;
  }
  port-mirror {
    disable-all-instances; /* Disable all port-mirroring instances */
    disable; /* Disable the global instance */
    input {
      rate 10; # start mirroring every 10th packet
      run-length 4; # mirror 4 additional packets
    }
    family inet {
      output {
        next-hop-group inet_nhg;
      }
    }
    family vpls {
      output {
        next-hop-group vpls_nhg;
      }
    }
    instance {
      inst1 {
        disable; /* Disable this instance */
        input {
          rate 1;
          maximum-packet-length 200;
        }
        family inet {
          output {
            next-hop-group inet_nhg;
          }
        }
      }
    }
  }
}
```

```

    }
  }
  family vpls {
    output {
      next-hop-group vpls_nhg_2;
    }
  }
}
}
}
}
}
}
}
}

```

The following example shows configuration of port mirroring using next-hops groups or multipacket port mirroring on a T series router:

```

forwarding-options {
  next-hop-group inet_nhg {
    group-type inet;
    interface so-0/0/0.0; # There is no need for the nexthop address on T series routers
    interface ge-2/0/2.0 {
      next-hop 1.2.3.4
    }
  }
  next-hop-subgroup sub_inet {
    interface so-1/2/0.0;
    interface ge-6/1/2.0 {
      next-hop 6.7.8.9;
    }
  }
  next-hop-group vpls_nhg_2 {
    group-type layer-2;
    interface ge-2/2/1.100;
    interface ge-2/3/9.0;
  }
}
port-mirroring {
  disable-all-instances; /*Disable all port-mirroring instances */
  disable; /* Disable the global instance */
  input {
    rate 10;
    run-length 4;
  }
  family inet {
    output {
      next-hop-group inet_nhg;
    }
  }
  family vpls {
    output {
      next-hop-group vpls_nhg;
    }
  }
}
instance {
  inst1 {
    disable; /* Disable this instance */
    input {
      rate 1;
    }
  }
}

```

```
        maximum-packet-length 200;
    }
    family inet {
        output {
            next-hop-group inet_nhg;
        }
    }
    family vpls {
        output {
            next-hop-group vpls_nhg_2;
        }
    }
}
}
```

The following example shows configuration of inline port mirroring using PM1 and PM2 as our port mirror instances.

```
instance {
    pm1 {
        input {
            rate 3;
        }
        family inet {
            output {
                interface ge-1/2/2.0 {
                    next-hop 40.0.0.2;
                }
            }
        }
    }
    pm2 {
        input-parameters-instance pm1;
        family inet {
            output {
                interface ge-1/2/3.0 {
                    next-hop 50.0.0.3;
                }
            }
        }
    }
}
}
firewall {
    filter pm_filter {
        term t1 {
            then port-mirror-instance pm2;
        }
    }
}
chassis {
    fpc 1 {
        port-mirror-instance pm1;
    }
}
```

The packets will be sampled at a rate of 3 and the copy is sent to 50.0.0.3.

**Related  
Documentation**

- *Understanding Port Mirroring*
- *Example: Multiple Port Mirroring with Next-Hop Groups Configuration*

## Load Balancing Among Multiple Monitoring Interfaces

The active monitoring application was initially intended for port-mirroring packets on an interface on a normal network router to single or multiple destinations. By port-mirroring these packets to a tunnel interface and using filter-based forwarding on the tunnel interface, port-mirrored packets can be load-balanced across set of interfaces. This method employs existing configuration statements for passive monitoring.

The configuration consists of the following parts; sample values are included for illustration only.

- Firewall filter configuration—Firewall filter PORT-MIRROR-TO-VT is used to port-mirror the packet to a Tunnel PIC, and filter **catch**, applied on the virtual tunnel (**vt**) interface, is used to send traffic to a filter-based routing instance.

```
[edit firewall]
filter PORT-MIRROR-TO-VT {
  term a {
    then {
      port-mirror;
      accept;
    }
  }
}
filter catch {
  term def {
    then {
      count counter;
      routing-instance fbf_instance;
    }
  }
}
```

For more information about firewall filters, see the *Routing Policy Feature Guide for Routing Devices*.

- Interface configuration—Apply filter PORT-MIRROR-TO-VT to the interface on which traffic is to be monitored actively.

```
[edit interfaces]
ge-1/3/0 {
  unit 0 {
    family inet {
      filter {
        input PORT-MIRROR-TO-VT;
      }
      address 10.38.0.2/30;
    }
  }
}
```

```
    }  
  }  
  vt-3/2/0 {  
    unit 0 {  
      family inet {  
        filter {  
          input catch;  
        }  
      }  
    }  
  }  
  mo-6/1/0 {  
    unit 0 {  
      family inet;  
    }  
  }  
  mo-6/2/0 {  
    unit 0 {  
      family inet;  
    }  
  }  
  mo-6/3/0 {  
    unit 0 {  
      family inet;  
    }  
  }  
  mo-7/1/0 {  
    unit 0 {  
      family inet;  
    }  
  }  
  mo-7/2/0 {  
    unit 0 {  
      family inet;  
    }  
  }  
  mo-7/3/0 {  
    unit 0 {  
      family inet;  
    }  
  }  
}
```

For more information on configuring interface properties, see the *Junos OS Network Interfaces Library for Routing Devices*.

- Routing instance configuration for filter-based forwarding:

```
[edit routing-instances fbf_instance]  
instance-type forwarding;  
routing-options {  
  static {  
    route 0.0.0.0/0 next-hop [ mo-7/1/0.0 mo-7/2/0.0 mo-7/3/0.0 mo-6/3/0.0  
      mo-6/2/0.0 mo-6/1/0.0 ];  
  }  
}
```

For more information on routing instance configuration, see the *Junos OS Routing Protocols Library for Routing Devices*.

- Routing table groups—Configure the routing table group to resolve the routes installed in the routing instances to directly connected next hops on the interface:

```
[edit routing-options]
interface-routes {
  rib-group inet common;
}
rib-groups {
  common {
    import-rib [ inet.0 fbf_instance.inet.0 ];
  }
}
forwarding-table {
  export pplb;
}
```

For more information on routing table groups, see the *Junos OS Routing Protocols Library for Routing Devices*.

- Policy for per-packet load balancing:

```
[edit policy-options]
policy-statement pplb {
  then {
    load-balance per-packet;
  }
}
```

For more information on routing policy groups, see the *Routing Policy Feature Guide for Routing Devices*.

- Port mirroring and monitoring groups—Configure the monitoring services options, and also define hash-based load balancing:

```
[edit forwarding-options]
port-mirroring {
  input {
    rate 1;
  }
  family inet {
    output {
      interface vt-3/2/0.0;
      no-filter-check;
    }
  }
}
monitoring group1 {
  family inet {
    output {
      export-format cflowd-version-5;
      flow-active-timeout 60;
      flow-inactive-timeout 15;
      cflowd 10.36.252.1 port 2055;
    }
  }
}
```

```
interface mo-6/1/0.0 {
  source-address 10.36.252.2;
}
interface mo-6/2/0.0 {
  source-address 10.36.252.2;
}
interface mo-6/3/0.0 {
  source-address 10.36.252.2;
}
interface mo-7/1/0.0 {
  source-address 10.36.252.2;
}
interface mo-7/2/0.0 {
  source-address 10.36.252.2;
}
interface mo-7/3/0.0 {
  source-address 10.36.252.2;
}
}
}
}
hash-key {
  family inet {
    layer-3;
  }
}
```

For more information on hash keys, see the *Routing Policy Feature Guide for Routing Devices*.

---

## Configuring Discard Accounting

Discard accounting is similar to traffic sampling, but varies from it in two ways:

- In discard accounting, the packet is intercepted by the monitoring PIC and is not forwarded to its destination.
- Traffic sampling allows you to limit the number of packets sampled by configuring the **max-packets-per-second**, **rate**, and **run-length** statements. Discard accounting does not provide these options, and a high packet count can potentially overwhelm the monitoring PIC.

A discard instance is a named entity that specifies collector information under the **accounting *name*** statement. Discard instances are referenced in firewall filter **term** statements by including the **then discard accounting *name*** statement.

Most of the other statements are also found at the **[edit forwarding-options sampling]** hierarchy level. For information on cflowd, see [“Enabling Flow Aggregation” on page 1151](#). The **flow-active-timeout** and **flow-inactive-timeout** statements are described in [“Configuring Flow Monitoring” on page 1144](#).

To direct sampled traffic to a flow-monitoring interface, include the **interface** statement. The **engine-id** and **engine-type** statements specify the accounting interface used on the traffic, and the **source-address** statement specifies the traffic source.

You cannot use rate-limiting with discard accounting; however, you can specify the duration of the interval for exporting aggregated accounting information by including the **aggregate-export-interval** statement in the configuration. This enables you to put a boundary on the amount of traffic exported to a flow-monitoring interface.

- Related Documentation**
- [Enabling Flow Aggregation on page 1151](#)
  - [Configuring Flow Monitoring on page 1144](#)

---

## Enabling Passive Flow Monitoring

You can monitor IPv4 traffic from another router if you have the following components installed in an M Series, MX Series, or T Series router:

- Monitoring Services, Adaptive Services, or Multiservices PICs to perform the service processing
- SONET/SDH, Fast Ethernet, or Gigabit Ethernet PICs as transit interface

On SONET/SDH interfaces, you enable passive flow monitoring by including the **passive-monitor-mode** statement at the **[edit interfaces so-fpc/pic/port unit logical-unit-number]** hierarchy level:

```
[edit interfaces so-fpc/pic/port unit logical-unit-number]  
passive-monitor-mode;
```

On Asynchronous Transfer Mode (ATM), Fast Ethernet, or Gigabit Ethernet interfaces, you enable passive flow monitoring by including the **passive-monitor-mode** statement at the **[edit interfaces interface-name]** hierarchy level:

```
[edit interfaces interface-name]  
passive-monitor-mode;
```

IPv6 passive monitoring is not supported on Monitoring Services PICs. You must configure port mirroring to forward the packets from the passive monitored ports to other interfaces. Interfaces configured on the following FPCs and PIC support IPv6 passive monitoring on the T640 and T1600 routers:

- Enhanced Scaling FPC2
- Enhanced Scaling FPC3
- Enhanced II FPC1
- Enhanced II FPC2
- Enhanced II FPC3
- Enhanced Scaling FPC4
- Enhanced Scaling FPC4.1
- 4-port 10-Gigabit Ethernet LAN/WAN PIC with XFP (supported on both WAN-PHY and LAN-PHY mode for both IPv4 and IPv6 addresses)
- Gigabit Ethernet PIC with SFP

- 10-Gigabit Ethernet PIC with XENPAK (T1600 router)
- SONET/SDH OC192/STM64 PIC (T1600 router)
- SONET/SDH OC192/STM64 PICs with XFP (T1600 router)
- SONET/SDH OC48c/STM16 PIC with SFP (T1600 router)
- SONET/SDH OC48/STM16 (Multi-Rate)
- SONET/SDH OC12/STM4 (Multi-Rate) PIC with SFP
- Type 1 SONET/SDH OC3/STM1 (Multi-Rate) PIC with SFP

To configure port mirroring, include the **port-mirroring** statement at the **[edit forwarding-options]** hierarchy level.

When you configure an interface in passive monitoring mode, the Packet Forwarding Engine silently drops packets coming from that interface and destined to the router itself. Passive monitoring mode also stops the Routing Engine from transmitting any packet from that interface. Packets received from the monitored interface can be forwarded to monitoring interfaces. If you include the **passive-monitor-mode** statement in the configuration:

- The ATM interface is always up, and the interface does not receive or transmit incoming control packets, such as Operation, Administration, and Maintenance (OAM) and Interim Local Management Interface (ILMI) cells.
- The SONET/SDH interface does not send keepalives or alarms and does not participate actively on the network.
- Gigabit and Fast Ethernet interfaces can support both per-port passive monitoring and per-VLAN passive monitoring. The destination MAC filter on the receive port of the Ethernet interfaces is disabled.
- Ethernet encapsulation options are not allowed.
- Ethernet interfaces do not support the **stacked-vlan-tagging** statement for both IPv4 and IPv6 packets in passive monitoring mode.

On monitoring services interfaces, you enable passive flow monitoring by including the **family** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level, specifying the **inet** option:

```
[edit interfaces interface-name unit logical-unit-number]  
family inet;
```

For the monitoring services interface, you can configure multiservice physical interface properties. For more information, see [“Configuring Flow-Monitoring Interfaces” on page 1144](#).

For conformity with the cflowd record structure, you must include the **receive-options-packets** and **receive-ttl-exceeded** statements at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet]** hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet]  
receive-options-packets;  
receive-ttl-exceeded;
```

For more information, see the following sections:

- [Passive Flow Monitoring for MPLS Encapsulated Packets on page 1205](#)
- [Example: Enabling IPv4 Passive Flow Monitoring on page 1206](#)
- [Example: Enabling IPv6 Passive Flow Monitoring on page 1208](#)

## Passive Flow Monitoring for MPLS Encapsulated Packets

On monitoring services interfaces, you can process MPLS packets that have not been assigned label values and have no corresponding entry in the **mpls.0** routing table. This allows you to assign a default route to unlabeled MPLS packets.

To configure a default label value for MPLS packets, include the **default-route** statement at the **[edit protocols mpls interface *interface-name* label-map]** hierarchy level:

```
[edit protocols mpls interface interface-name label-map]
default-route {
  (next-hop (address | interface-name | address/interface-name)) | (reject | discard);
  (pop | (swap <out-label>));
  class-of-service value;
  preference preference;
  type type;
}
```

For more information about static labels, see the *Junos OS MPLS Applications Library for Routing Devices*.

## Removing MPLS Labels from Incoming Packets

The Junos OS can forward only IPv4 packets to a Monitoring Services, Adaptive Services, or Multiservices PIC. IPv4 and IPv6 packets with MPLS labels cannot be forwarded to a monitoring PIC. By default, if packets with MPLS labels are forwarded to the monitoring PIC, they are discarded. To monitor IPv4 and IPv6 packets with MPLS labels, you must remove the MPLS labels as the packets arrive on the interface.

You can remove up to two MPLS labels from an incoming packet by including the **pop-all-labels** statement at the **[edit interfaces *interface-name* (atm-options | fastether-options | gige-ther-options | sonet-options) mpls]** hierarchy level:

```
[edit interfaces interface-name (atm-options | fastether-options | gige-ther-options |
sonet-options) mpls]
pop-all-labels {
  required-depth [ numbers ];
}
```

By default, the **pop-all-labels** statement takes effect for incoming packets with one or two labels. You can specify the number of MPLS labels that an incoming packet must have for the **pop-all-labels** statement to take effect by including the **required-depth** statement at the **[edit interfaces *interface-name* (atm-options | fastether-options | gige-ther-options | sonet-options) mpls pop-all-labels]** hierarchy level:

```
[edit interfaces interface-name (atm-options | fastether-options | gige-ther-options |
sonet-options) mpls pop-all-labels]
required-depth [ numbers ];
```

The required depth can be 1, 2, or [ 1 2 ]. If you include the **required-depth 1** statement, the **pop-all-labels** statement takes effect for incoming packets with one label only. If you include the **required-depth 2** statement, the **pop-all-labels** statement takes effect for incoming packets with two labels only. If you include the **required-depth [ 1 2 ]** statement, the **pop-all-labels** statement takes effect for incoming packets with one or two labels. A required depth of [ 1 2 ] is equivalent to the default behavior of the **pop-all-labels** statement.

When you remove MPLS labels from incoming packets, note the following:

- The **pop-all-labels** statement has no effect on IP packets with three or more MPLS labels.
- When you enable MPLS label removal, you must configure all ports on a PIC with the same label popping mode and required depth.
- You use the **pop-all-labels** statement to enable passive monitoring applications, not active monitoring applications.
- You cannot apply MPLS filters or accounting to the MPLS labels because the labels are removed as soon as the packet arrives on the interface.
- On ATM2 interfaces, you must use a label value greater than 4095 because the lower range of MPLS labels is reserved for label-switched interface (LSI) and virtual private LAN service (VPLS) support. For more information, see the *Junos OS VPNs Library for Routing Devices*.
- The following ATM encapsulation types are not supported on interfaces with MPLS label removal:
  - **atm-ccc-cell-relay**
  - **atm-ccc-vc-mux**
  - **atm-mlppp-llc**
  - **atm-tcc-snap**
  - **atm-tcc-vc-mux**
  - **ether-over-atm-llc**
  - **ether-vpls-over-atm-llc**

### Example: Enabling IPv4 Passive Flow Monitoring

The following example shows a complete configuration for enabling passive flow monitoring on an Ethernet interface.

In this example, the Gigabit Ethernet interface can accept all Ethernet packets. It strips VLAN tags (if there are any) and up to two MPLS labels blindly, and passes IPv4 packets to the monitoring interface. With this configuration, it can monitor IPv4, VLAN+IPv4, VLAN+MPLS+IPv4, and VLAN+MPLS+MPLS+IPv4 labeled packets.

The Fast Ethernet interface can accept only packets with VLAN ID 100. All other packets are dropped. With this configuration, it can monitor VLAN (ID=100)+IPv4, VLAN (ID=100)+MPLS+IPv4, and VLAN (ID=100)+MPLS+MPLS+IPv4 labeled packets.

```
[edit firewall]
family inet {
  filter input-monitoring-filter {
    term def {
      then {
        count counter;
        accept;
      }
    }
  }
}
[edit interfaces]
ge-0/0/0 {
  passive-monitor-mode;
  gigether-options {
    mpls {
      pop-all-labels;
    }
  }
  unit 0 {
    family inet {
      filter {
        input input-monitoring-filter;
      }
    }
  }
}
fe-0/1/0 {
  passive-monitor-mode;
  vlan-tagging;
  fastether-options {
    mpls {
      pop-all-labels required-depth [ 1 2 ];
    }
  }
  unit 0 {
    vlan-id 100;
    family inet {
      filter {
        input input-monitoring-filter;
      }
    }
  }
}
mo-1/0/0 {
  unit 0 {
    family inet {
      receive-options-packets;
      receive-ttl-exceeded;
    }
  }
}
```

```
    unit 1 {
        family inet;
    }
}
[edit forwarding-options]
monitoring mon1 {
    family inet {
        output {
            export-format cflowd-version-5;
            cflowd 50.0.0.2 port 2055;
            interface mo-1/0/0.0 {
                source-address 50.0.0.1;
            }
        }
    }
}
[edit routing-instances]
monitoring-vrf {
    instance-type vrf;
    interface ge-0/0/0.0;
    interface fe-0/1/0.0;
    interface mo-1/0/0.1;
    route-distinguisher 68:1;
    vrf-import monitoring-vrf-import;
    vrf-export monitoring-vrf-export;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop mo-1/0/0.1;
        }
    }
}
[edit policy-options]
policy-statement monitoring-vrf-import {
    then {
        reject;
    }
}
policy-statement monitoring-vrf-export {
    then {
        reject;
    }
}
```

### Example: Enabling IPv6 Passive Flow Monitoring

The following example shows a complete configuration for enabling IPv6 passive flow monitoring on an Ethernet interface.

In this example, the Gigabit Ethernet interface can accept all Ethernet packets. It strips VLAN tags (if there are any) and up to two MPLS labels blindly, and passes IPv6 packets to the monitoring interface. With this configuration, the Gigabit Ethernet interface can monitor IPv6, VLAN+IPv6, VLAN+MPLS+IPv6, and VLAN+MPLS+MPLS+IPv6 labeled packets.

The vlan-tagged Gigabit Ethernet interface can accept only packets with VLAN ID 100. All other packets are dropped. With this configuration, it can monitor VLAN (ID=100)+IPv6, VLAN (ID=100)+MPLS+IPv6, and VLAN (ID=100)+MPLS+MPLS+IPv6 labeled packets.

```
[edit interfaces]
xe-0/1/0 {
  passive-monitor-mode;
  unit 0 {
    family inet6 {
      filter {
        input port-mirror6;
      }
      address 2001::1/128;
    }
  }
}
xe-0/1/2 {
  passive-monitor-mode;
  vlan-tagging;
  unit 0 {
    vlan-id 100;
    family inet6 {
      filter {
        input port-mirror6;
      }
    }
  }
}
xe-0/1/1 {
  unit 0 {
    family inet6 {
      address 2000::1/128;
    }
  }
}
[edit firewall]
family inet6 {
  filter port-mirror6 {
    term term2 {
      then {
        count count_pm;
        port-mirror;
        accept;
      }
    }
  }
}
[edit forwarding options]
port-mirroring {
  input {
    rate 1;
  }
  family inet6 {
    output {
      interface xe-0/1/1.0 {
```

```

        next-hop 2000::3;
    }
    no-filter-check;
}
}
}

```

**Related Documentation**

- [Passive Flow Monitoring Overview on page 1124](#)

## Configuring Services Interface Redundancy with Flow Monitoring

Active monitoring services configurations on AS, Multiservices PICs, and Multiservices DPCs support redundancy. To configure redundancy, you specify a redundancy services PIC (**rsp**) interface in which the primary AS or Multiservices PIC is active and a secondary PIC is on standby. If the primary PIC fails, the secondary PIC becomes active, and all service processing is transferred to it. If the primary PIC is restored, it remains on standby and does not preempt the secondary PIC; you need to manually restore the services to the primary PIC. To determine which PIC is currently active, issue the **show interfaces redundancy** command.



**NOTE:** On flow-monitoring configurations, the only service option supported is *warm standby*, in which one backup PIC supports multiple working PICs. Recovery times are not guaranteed, because the configuration must be completely restored on the backup PIC after a failure is detected. However, configuration is preserved and available on the new active PIC.

As with the other services that support warm standby, you can issue the **request interfaces (revert | switchover)** command to switch manually between the primary and secondary flow monitoring interfaces.

For more information, see “[Configuring AS or Multiservices PIC Redundancy](#)” on page 806. For information on operational mode commands, see the [CLI Explorer](#).

A sample configuration follows.

```

interface {
  rsp0 {
    redundancy-options {
      primary sp-0/0/0;
      secondary sp-1/3/0;
    }
    unit 0 {
      family inet;
    }
  }
}
interface {
  ge-0/2/0 {
    unit 0 {
      family inet {

```

```

        filter {
            input as_sample;
        }
    }
    address 10.58.255.49/28;
}
}
forwarding-options {
    sampling {
        instance instance1 { # named instances of sampling parameters
            input {
                rate 1;
                run-length 0;
                max-packets-per-second 65535;
            }
            family inet {
                output {
                    flow-server 10.10.10.2 {
                        port 5000;
                        version 5;
                    }
                    flow-active-timeout 60;
                    interface rsp0 {
                        source-address 10.10.10.1;
                    }
                }
            }
        }
    }
}
firewall {
    filter as_sample {
        term t1 {
            then {
                sample;
                accept;
            }
        }
    }
}
}

```

**Related  
Documentation**

- [Active Flow Monitoring Overview on page 1125](#)
- [Configuring Flow Monitoring on page 1144](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 1182](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 1148](#)



# Summary of Flow-Monitoring Configuration Statements

The following sections explain each of the flow-monitoring configuration statements. The statements are organized alphabetically.

- [accounting on page 1216](#)
- [address \(Interfaces\) on page 1217](#)
- [aggregate-export-interval on page 1217](#)
- [aggregation on page 1218](#)
- [autonomous-system-type on page 1219](#)
- [core-dump on page 1222](#)
- [destination \(Tunnel Remote End\) on page 1223](#)
- [disable \(Forwarding Options\) on page 1223](#)
- [disable-all-instances on page 1224](#)
- [engine-id \(Forwarding Options\) on page 1224](#)
- [engine-type on page 1225](#)
- [extension-service on page 1226](#)
- [export-format on page 1227](#)
- [filename on page 1234](#)
- [files on page 1235](#)
- [filter on page 1236](#)
- [flow-active-timeout on page 1237](#)
- [flow-export-rate on page 1238](#)
- [flow-control-options on page 1238](#)
- [flow-export-destination on page 1239](#)
- [flow-inactive-timeout on page 1240](#)
- [flow-monitoring on page 1241](#)
- [flow-server on page 1242](#)
- [forwarding-options on page 1243](#)

- [inline-jflow](#) on page 1243
- [input-interface-index](#) on page 1245
- [interfaces](#) on page 1251
- [ipv4-template](#) on page 1251
- [ipv6-template](#) on page 1252
- [label-position](#) on page 1252
- [local-dump](#) on page 1253
- [match](#) on page 1253
- [maximum-packet-length](#) on page 1254
- [max-packets-per-second](#) on page 1255
- [monitoring](#) on page 1256
- [mpls-ipv4-template](#) on page 1257
- [mpls-template](#) on page 1257
- [multiservice-options](#) on page 1258
- [next-hop \(Forwarding Options\)](#) on page 1258
- [no-core-dump](#) on page 1260
- [no-filter-check](#) on page 1260
- [no-local-dump](#) on page 1260
- [no-remote-trace \(Trace Options\)](#) on page 1261
- [no-stamp](#) on page 1261
- [no-syslog](#) on page 1261
- [no-world-readable](#) on page 1261
- [observation-domain-id](#) on page 1262
- [option-refresh-rate](#) on page 1263
- [options-template-id](#) on page 1264
- [output-interface-index](#) on page 1269
- [passive-monitor-mode](#) on page 1270
- [pop-all-labels](#) on page 1271
- [port](#) on page 1272
- [port-mirroring](#) on page 1273
- [rate \(Forwarding Options\)](#) on page 1274
- [receive-options-packets](#) on page 1274
- [receive-ttl-exceeded](#) on page 1275
- [required-depth](#) on page 1275
- [run-length](#) on page 1276
- [sample-once](#) on page 1276
- [services](#) on page 1281

- [size](#) on page 1281
- [source-address \(Forwarding Options\)](#) on page 1282
- [source-id](#) on page 1282
- [stamp](#) on page 1283
- [syslog](#) on page 1283
- [template-id](#) on page 1286
- [template-refresh-rate](#) on page 1287
- [traceoptions \(Forwarding Options\)](#) on page 1287
- [unit](#) on page 1288
- [version](#) on page 1289
- [world-readable](#) on page 1293

## accounting

---

**Syntax**    `accounting name {  
          output {  
            aggregate-export-interval seconds;  
            cflowd hostname {  
              aggregation {  
                autonomous-system;  
                destination-prefix;  
                protocol-port;  
                source-destination-prefix {  
                  caida-compliant;  
                }  
                source-prefix;  
              }  
            }  
            autonomous-system-type (origin | peer);  
            port port-number;  
            version format;  
          }  
          flow-active-timeout seconds;  
          flow-inactive-timeout seconds;  
          interface interface-name {  
            engine-id (Forwarding Options) number;  
            engine-type number;  
            source-address (Forwarding Options) address;  
          }  
          }  
          }  
          }`

**Hierarchy Level**    [edit [forwarding-options](#)]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Specify the discard accounting instance name and options.

The statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring Discard Accounting on page 1202](#)

## address (Interfaces)

<b>Syntax</b>	<code>address address {     destination address; }</code>
<b>Hierarchy Level</b>	[edit <code>interfaces interface-name unit logical-unit-number family family</code> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the interface address.
<b>Options</b>	<p><b>address</b>—Address of the interface.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other options not associated with flow monitoring.</li> <li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> </ul>

## aggregate-export-interval

<b>Syntax</b>	<code>aggregate-export-interval seconds;</code>
<b>Hierarchy Level</b>	[edit <code>forwarding-options accounting name output</code> ], [edit <code>forwarding-options sampling instance instance-name family (inet   inet6   mpls) output</code> ], [edit <code>forwarding-options sampling family (inet   inet6   mpls) output</code> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the duration, in seconds, of the interval for exporting aggregate accounting information.
<b>Options</b>	<b>seconds</b> —Duration.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Discard Accounting on page 1202</a></li> </ul>

## aggregation

---

<b>Syntax</b>	<pre>aggregation {     autonomous-system;     destination-prefix;     protocol-port;     source-destination-prefix {         caida-compliant;     }     source-prefix; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options accounting output cflowd hostname</a> ], [edit <a href="#">forwarding-options sampling instance instance-name family</a> (inet   inet6   mpls) <a href="#">output flow-server hostname</a> ], [edit <a href="#">forwarding-options sampling family</a> (inet   inet6   mpls) <a href="#">output flow-server hostname</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For cflowd version 8 only, specify the type of data to be aggregated; cflowd records and sends only those flows that match the specified criteria.
<b>Options</b>	<p><b>autonomous-system</b>—Aggregate by autonomous system (AS) number.</p> <p><b>caida-compliant</b>—Record source and destination mask-length values in compliance with the Version 2.1b1 release of CAIDA's cflowd application. If this statement is not configured, the Junos OS records source and destination mask length values in compliance with the <i>cflowd Configuration Guide</i>, dated August 30, 1999.</p> <p><b>destination-prefix</b>—Aggregate by destination prefix.</p> <p><b>protocol-port</b>—Aggregate by protocol and port number.</p> <p><b>source-destination-prefix</b>—Aggregate by source and destination prefix.</p> <p><b>source-prefix</b>—Aggregate by source prefix.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Enabling Flow Aggregation on page 1151</a></li></ul>

## autonomous-system-type

---

<b>Syntax</b>	<code>autonomous-system-type (origin   peer);</code>
<b>Hierarchy Level</b>	[edit <code>forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output flow-server <i>hostname</i></code> ], [edit <code>forwarding-options sampling family (inet   inet6   mpls) output flow-server <i>hostname</i></code> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the type of AS numbers that cflowd exports.
<b>Default</b>	<code>origin</code>
<b>Options</b>	<p><code>origin</code>—Export origin AS numbers of the packet source address in the Source Autonomous System cflowd field.</p> <p><code>peer</code>—Export peer AS numbers through which the packet passed in the Source Autonomous System cflowd field.</p>
<b>Required Privilege Level</b>	<p><code>interface</code>—To view this statement in the configuration.</p> <p><code>interface-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Enabling Flow Aggregation on page 1151</a></li> </ul>

## cflowd

---

See the following sections:

- [cflowd \(Discard Accounting\) on page 1220](#)
- [cflowd \(Flow Monitoring\) on page 1221](#)

### cflowd (Discard Accounting)

**Syntax** `cflowd hostname {  
    aggregation {  
        autonomous-system;  
        destination-prefix;  
        protocol-port;  
        source-destination-prefix {  
            caida-compliant;  
        }  
        source-prefix;  
    }  
    autonomous-system-type (origin | peer);  
    label-position {  
        template template-name;  
    }  
    (local-dump | no-local-dump);  
    port port-number;  
    source-address (Forwarding Options) address;  
    version format;  
}`

**Hierarchy Level** [edit [forwarding-options accounting \*name\* output](#)],

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Collect an aggregate of sampled flows and send the aggregate to a specified host system that runs the collection utility `cfcollect`.

You can configure up to one version 5 and one version 8 flow format at the [edit [forwarding-options accounting \*name\* output](#)] hierarchy level.

**Options** *hostname*—The IP address or identifier of the host system (the workstation running the `cflowd` utility).

The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**


- [Enabling Flow Aggregation on page 1151](#)

## cflowd (Flow Monitoring)

<b>Syntax</b>	<pre>cflowd hostname {   port port-number; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options monitoring name</a> inet <a href="#">output</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Collect an aggregate of sampled flows and send the aggregate to a specified host system that runs the collection utility cfdcollect.</p> <p>You can configure up to eight version 5 flow formats at the [edit <a href="#">forwarding-options monitoring name output</a>] hierarchy level. Version 8 flow formats are not supported for flow-monitoring applications.</p>
<b>Options</b>	<p><b>hostname</b>—The IP address or identifier of the host system (the workstation running the cflowd utility).</p> <p>The remaining statement is explained separately.</p>
<b>Usage Guidelines</b>	See “ <a href="#">Enabling Flow Aggregation</a> ” on page 1151.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

## core-dump

---

Syntax	(core-dump   no-core-dump);
Hierarchy Level	[edit <a href="#">interfaces</a> mo-fpc/pic/port <a href="#">multiservice-options</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>A useful tool for isolating the cause of a problem. Core dumping is enabled by default. The directory <b>/var/tmp</b> contains core files. The Junos OS saves the current core file (0) and the four previous core files, which are numbered from 1 through 4 (from newest to oldest):</p> <div> <b>NOTE:</b> By default, all members of a configured user group (with read-only permissions) can access the core dump files and attach them to cases associated with JTAC.</div>
	<ul style="list-style-type: none"><li>• <b>core-dump</b>—Enable the core dumping operation.</li><li>• <b>no-core-dump</b>—Disable the core dumping operation.</li></ul>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li></ul>

## destination (Tunnel Remote End)

<b>Syntax</b>	<code>destination address;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
<b>Description</b>	For tunnel interfaces, specify the remote address of the tunnel.
<b>Options</b>	<b><i>destination-address</i></b> —Address of the remote side of the connection.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Unicast Tunnels on page 1567</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> <li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li> </ul>

## disable (Forwarding Options)

<b>Syntax</b>	<code>disable;</code>
<b>Hierarchy Level</b>	[edit forwarding-options port-mirror], [edit forwarding-options port-mirror instance <i>instance-name</i> ], [edit <b>forwarding-options</b> <b>sampling</b> ], [edit <b>forwarding-options</b> <b>sampling</b> instance <i>instance-name</i> ], [edit <b>forwarding-options</b> <b>sampling</b> family (inet   inet6   mpls) ], [edit <b>forwarding-options</b> <b>sampling</b> family (inet   inet6   mpls) <b>output file</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement added to <b>port-mirror</b> hierarchy in Junos OS Release 9.6.
<b>Description</b>	Disable traffic accounting, port mirroring, or sampling.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> <li>• <a href="#">Configuring Port Mirroring on page 1186</a></li> </ul>

## disable-all-instances

---


<b>Syntax</b>	disable-all-instances;
<b>Hierarchy Level</b>	[edit forwarding-options port-mirror]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Disable all port mirroring instances globally.
<b>Usage Guidelines</b>	See “Configuring Port Mirroring” on page 1186.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.

## engine-id (Forwarding Options)

---


<b>Syntax</b>	engine-id <i>number</i> ;
<b>Hierarchy Level</b>	[edit forwarding-options accounting <i>name</i> output interface <i>interface-name</i> ], [edit forwarding-options monitoring <i>name</i> output interface <i>interface-name</i> ], [edit forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output interface <i>interface-name</i> ], [edit forwarding-options sampling family (inet   inet6   mpls) output interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the engine ID number for flow monitoring and accounting services.
<b>Options</b>	<i>number</i> —Identity of accounting interface.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li><li>• <a href="#">Configuring Discard Accounting on page 1202</a></li></ul>

## engine-type

<b>Syntax</b>	<code>engine-type <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit forwarding-options accounting <i>name</i> output interface <i>interface-name</i>],</code> <code>[edit forwarding-options monitoring <i>name</i> output interface <i>interface-name</i>],</code> <code>[edit forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output</code> <code>interface <i>interface-name</i>],</code> <code>[edit forwarding-options sampling family (inet   inet6   mpls) output interface <i>interface-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Specify the engine type number for flow monitoring and accounting services. The engine type attribute refers to the type of the flow switching engine, such as the route processor or a line module. The configured engine type is inserted in output <b>cflowd</b> packets. The <b>Source ID</b>, a 32-bit value to ensure uniqueness for all flows exported from a particular device, is the equivalent of the engine type and the engine ID fields.</p>
<div>  <p><b>NOTE:</b> You must configure a source address in the output interface statements. The interface-level statement of engine-type is added automatically but you may override this value with manually configured statements to track different flows with a single cflowd collector.</p> </div>	
<b>Options</b>	<i>number</i> —Platform-specific accounting interface type.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> <li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li> <li>• <a href="#">Configuring Discard Accounting on page 1202</a></li> </ul>

## extension-service

---

<b>Syntax</b>	<pre>extension-service service-name {     provider-specific rules; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options sampling instance</a> <i>instance-name</i> <a href="#">family</a> (inet  inet6) <a href="#">output</a> ] [edit <a href="#">forwarding-options sampling family</a> (inet  inet6) <a href="#">output</a> ] [edit services service-set <i>service-set-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<p>Define a customer specific sampling configuration.</p> <p>Define a service set or traffic monitoring for applications using application-specific configuration guidelines.</p>
	<div> <b>NOTE:</b> If the <code>extension-service</code> statement is specified while configuring a service set, the <code>service-order</code> statement is mandatory.</div>
<b>Options</b>	<p><i>provider-specific rules</i>—Provider-specific subhierarchy for services and service sets. See the application-specific documentation for details.</p> <p><i>service-name</i>—Name of the service.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">service-order</a></li><li>• <a href="#">sampling on page 1278</a></li></ul>

## export-format

---

<b>Syntax</b>	<code>export-format <i>format</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options monitoring name output</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Flow monitoring export format.
<b>Options</b>	<i>format</i> —Format of the flows. <b>Values:</b> 5 or 8 <b>Default:</b> 5
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">version on page 1289</a></li><li>• <a href="#">Exporting Flows on page 1146</a></li></ul>

## family

---

See the following sections:

- [family \(Interfaces\) on page 1228](#)
- [family \(Monitoring\) on page 1229](#)
- [family \(Port Mirroring\) on page 1230](#)
- [family \(Sampling\) on page 1231](#)

### family (Interfaces)

**Syntax**

```
family family {  
  address address {  
    destination destination-address;  
  }  
  filter {  
    group filter-group-number;  
    input filter-name;  
    output filter-name;  
  }  
  sampling direction;  
  receive-options-packets;  
  receive-ttl-exceeded;  
}
```

**Hierarchy Level** [edit interfaces *interface-name* [unit](#) *logical-unit-number*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure protocol family information for the logical interface.

**Options** *family*—Protocol family; for flow monitoring and accounting services, only the IP version 4 (IPv4) protocol (*inet*) is supported.

The remaining statements are explained separately.

**Usage Guidelines** See [“Configuring Flow Monitoring” on page 1144](#).

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Junos OS Network Interfaces Library for Routing Devices](#) for other options not used with services interfaces.

## family (Monitoring)

<b>Syntax</b>	<pre> family inet {   output {     flow-active-timeout seconds;     flow-inactive-timeout seconds;     export-format format;     cflowd hostname {       aggregation {         autonomous-system;         destination-prefix;         protocol-port;         source-destination-prefix {           caida-compliant;         }         source-prefix;       }       port port-number;     }     interface interface-name {       engine-id number;       engine-type number;       input-interface-index number;       output-interface-index number;       source-address address;     }   } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options monitoring name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Specify input and output interfaces and properties for flow monitoring. Only IPv4 (<a href="#">inet</a>) is supported.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li> </ul>

## family (Port Mirroring)

**Syntax**    family (inet | inet6) {  
              output {  
                  interface *interface-name* {  
                      next-hop *address*;  
                  }  
              no-filter-check;  
          }

**Hierarchy Level**    [edit [forwarding-options port-mirroring](#)]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure the protocol family to be sampled. Only IPv4 (**inet**) and IPv6 (**inet6**) are supported.

                  The statements are explained separately.

**Usage Guidelines**    See “[Configuring Port Mirroring](#)” on page 1186.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

## family (Sampling)

Syntax	<pre> family (inet   inet6   mpls) {   disable;   output {     aggregate-export-interval seconds;     flow-active-timeout seconds;     flow-inactive-timeout seconds;     extension-service service-name;     flow-server hostname {       aggregation {         autonomous-system;         destination-prefix;         protocol-port;         source-destination-prefix {           caida-compliant;         }         source-prefix;       }       autonomous-system-type (origin   peer);       (local-dump   no-local-dump);       port port-number;       source-address address;       version format;       version9 {         template template-name;       }     }   }   interface interface-name {     engine-id number;     engine-type number;     source-address address;   }   file {     disable;     filename filename;     files number;     size bytes;     (stamp   no-stamp);     (world-readable   no-world-readable);   }   inline-jflow {     source-address address;     flow-export-rate rate;   } } </pre>
Hierarchy Level	<p>[edit forwarding-options sampling],</p> <p>[edit forwarding-options sampling instance instance-name]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p><b>mpls</b> option introduced in Release 8.3.</p> <p><b>inet6</b> option introduced in Release 9.4.</p>

**Description** Configure the protocol family to be sampled. IPv4 (**inet**) is supported for most purposes, but you can configure **family mpls** to collect and export MPLS label information or **family inet6** to collect and export IPv6 traffic using flow aggregation version 9.

The remaining statements are explained separately.



**NOTE:** The `inline-jflow` statement is valid only under the `[edit forwarding-options sampling instance instance-name family inet output]` hierarchy level. The `file` statement is valid only under the `[edit forwarding-options sampling family inet output]` hierarchy level.

---

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Traffic Sampling on page 1134](#)

## file

---

See the following sections:

- [file \(Sampling\) on page 1233](#)
- [file \(Trace Options\) on page 1234](#)

### file (Sampling)

**Syntax**

```
file {
  disable;
  filename filename;
  files number;
  size bytes;
  (stamp | no-stamp);
  (world-readable | no-world-readable);
}
```

**Hierarchy Level** [edit [forwarding-options sampling family inet output](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Collect the traffic samples in a file.

The statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Traffic Sampling on page 1134](#)

## file (Trace Options)

Syntax	file <i>filename</i> <files number <size bytes> <world-readable   no-world-readable>;
Hierarchy Level	[edit <a href="#">forwarding-options port-mirroring traceoptions</a> ], [edit <a href="#">forwarding-options sampling traceoptions</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure information about the files that contain trace logging information.
Options	<i>filename</i> —The name of the file containing the trace information. <b>Default:</b> /var/log/sampled  The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Tracing Traffic Sampling Operations on page 1140</a></li></ul>

---

## filename

Syntax	filename <i>filename</i> ;
Hierarchy Level	[edit <a href="#">forwarding-options sampling family</a> (inet   inet6   impls) <a href="#">output file</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the name of the output file.
Options	<i>filename</i> —Name of the file in which to place the traffic samples. All files are placed in the directory /var/tmp.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li></ul>

## files

---



<b>Syntax</b>	<code>files <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options port-mirroring traceoptions file</a> ], [edit <a href="#">forwarding-options sampling family</a> (inet   inet6   mpls) <a href="#">output file</a> ], [edit <a href="#">forwarding-options sampling traceoptions file</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the total number of files to be saved with samples or trace data.
<b>Options</b>	<p><b><i>number</i></b>—Maximum number of traffic sampling or trace log files. When a file named <b><i>sampling-file</i></b> reaches its maximum size, it is renamed <b><i>sampling-file.0</i></b>, then <b><i>sampling-file.1</i></b>, and so on, until the maximum number of traffic sampling files is reached. Then the oldest sampling file is overwritten.</p> <p><b>Range:</b> 1 through 100 files</p> <p><b>Default:</b> 5 files for sampling output; 10 files for trace log information</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Port Mirroring on page 1186</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> </ul>

## filter

---

<b>Syntax</b>	<pre>filter {     input <i>filter-name</i>;     output <i>filter-name</i>;     group <i>filter-group-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> <a href="#">unit</a> <i>logical-unit-number</i> <a href="#">family</a> inet]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Apply a firewall filter to an interface. You can also use filters for encrypted traffic.
<b>Options</b>	<p><b>group <i>filter-group-number</i></b>—Define an interface to be part of a filter group. The default filter group number is 0.</p> <p><b>input <i>filter-name</i></b>—Name of one filter to evaluate when packets are received on the interface.</p> <p><b>output <i>filter-name</i></b>—Name of one filter to evaluate when packets are transmitted on the interface.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Routing Policy Feature Guide for Routing Devices</i> or the <i>Junos OS Administration Library for Routing Devices</i></li><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li></ul>

## flow-active-timeout

<b>Syntax</b>	<code>flow-active-timeout seconds;</code>
<b>Hierarchy Level</b>	<code>[edit forwarding-options accounting name output],</code> <code>[edit forwarding-options monitoring name output],</code> <code>[edit forwarding-options sampling instance instance-name family (inet   inet6   mpls) output],</code> <code>[edit forwarding-options sampling family (inet   inet6   mpls) output],</code> <code>[edit services flow-monitoring version9]</code> <code>[edit services flow-monitoring version-ipfix template template-name]</code>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Support at the <code>[edit services flow-monitoring version-ipfix template template-name]</code> hierarchy level added in Junos OS Release 10.2.</p>
<b>Description</b>	Set the interval after which an active flow is exported.
<div>  <p><b>NOTE:</b> The router must include an Adaptive Services, Multiservices, or Monitoring Services PIC for this statement to take effect.</p> </div>	
<b>Options</b>	<p><b>seconds</b>—Duration of the timeout period.</p> <p><b>Range:</b> 60 through 1800 seconds (for <b>forwarding-options</b> configurations); 10 through 600 seconds (for <b>services</b> configurations)</p> <p><b>Default:</b> 1800 seconds (for <b>forwarding-options</b> configurations); 60 seconds (for <b>services</b> configurations)</p>
<div>  <p><b>NOTE:</b> In active flow monitoring, the cflowd or flow monitoring version 9 records are exported after a time period that is a multiple of 60 seconds and greater than or equal to the configured active timeout value. For example, if the active timeout value is 90 seconds, the cflowd or flow monitoring version 9 records are exported at 120-second intervals. If the active timeout value is 150 seconds, the cflowd or flow monitoring version 9 records are exported at 180-second intervals, and so forth.</p> </div>	
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Time Periods when Flow Monitoring is Active and Inactive on page 1147</a></li> <li>• <a href="#">Configuring the Version 9 Template Properties on page 1157</a></li> </ul>

## flow-export-rate

---

<b>Syntax</b>	<code>flow-export-rate <i>rate</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options sampling instance <i>instance-name</i></a> <a href="#">family inet output inline-jflow</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the flow export rate of monitored packets in kpps.
<b>Options</b>	<i>rate</i> —Flow export rate of monitored packets in kpps (from 1 to 400).
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Discard Accounting on page 1202</a></li><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li></ul>

## flow-control-options

---

<b>Syntax</b>	<pre>flow-control-options {   down-on-flow-control;   dump-on-flow-control;   reset-on-flow-control; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces mo-fpc/pic/port multiservice-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 8.4.
<b>Description</b>	<p>Configure the flow control options for application recovery in case of a prolonged flow control failure.</p> <ul style="list-style-type: none"><li>• <b>down-on-flow-control</b>—Bring interface down during prolonged flow control.</li><li>• <b>dump-on-flow-control</b>—Cause core dump during prolonged flow control.</li><li>• <b>reset-on-flow-control</b>—Reset interface during prolonged flow control.</li></ul>
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Flow Monitoring</a> ” on page 1144.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.


## flow-export-destination

---

<b>Syntax</b>	<code>flow-export-destination {     (cflowd-collector   collector-pic); }</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options monitoring group-name</a> family inet <a href="#">output</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure flow collection.
<b>Options</b>	<code>cflowd-collector</code> —cflowd collector.  <code>collector-pic</code> —Collector PIC.
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Exporting Flows on page 1146</a></li></ul>

## flow-inactive-timeout

---

<b>Syntax</b>	<code>flow-inactive-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	<code>[edit forwarding-options accounting <i>name</i> output],</code> <code>[edit forwarding-options monitoring <i>name</i> output],</code> <code>[edit forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output],</code> <code>[edit forwarding-options sampling family (inet   inet6   mpls) output],</code> <code>[edit services flow-monitoring version 9]</code> <code>[edit services flow-monitoring version-ipfix template <i>template-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Support at the <code>[edit services flow-monitoring version-ipfix template <i>template-name</i>]</code> hierarchy level added in Junos OS Release 10.2.
<b>Description</b>	Set the interval of inactivity that marks a flow inactive.
<div> <b>NOTE:</b> The router must include an Adaptive Services, Multiservices, or Monitoring Services PIC for this statement to take effect.</div>	
<b>Options</b>	<b><i>seconds</i></b> —Duration of the timeout period. <b>Range:</b> 60 through 1800 seconds (for <b>forwarding-options</b> configurations); 10 through 600 seconds (for <b>services</b> configurations) <b>Default:</b> 1800 seconds (for <b>forwarding-options</b> configurations); 60 seconds (for <b>services</b> configurations)
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Time Periods when Flow Monitoring is Active and Inactive on page 1147</a></li><li>• <a href="#">Configuring the Version 9 Template Properties on page 1157</a></li></ul>

## flow-monitoring

```
Syntax  flow-monitoring {
        version9 {
            template template-name {
                options-template-id
                template-id
                source-id
                flow-active-timeout seconds;
                flow-inactive-timeout seconds;
                ipv4-template;
                ipv6-template;
                mpls-template {
                    label-position [ positions ];
                }
                mpls-ipv4-template {
                    label-position [ positions ];
                }
                peer-as-billing-template;
                option-refresh-rate packets packets seconds seconds;
                template-refresh-rate packets packets seconds seconds;
            }
        }
    }
```

**Hierarchy Level** [edit [services](#)]

**Release Information** Statement introduced in Junos OS Release 8.3.

**Description** Specify the active monitoring properties for flow aggregation version 9.

The statements are explained separately.

**Usage Guidelines** See “Configuring Flow Aggregation to Use Version 9 Flow Templates” on page 1156.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

## flow-server

Syntax	<pre> flow-server <i>hostname</i> {     aggregation {         autonomous-system;         destination-prefix;         protocol-port;         source-destination-prefix {             caida-compliant;         }         source-prefix;     }     autonomous-system-type (origin   peer);     (local-dump   no-local-dump);     port <i>port-number</i>;     source-address <i>address</i>;     version <i>format</i>;     version9 {         template <i>template-name</i>;     } } </pre>
Hierarchy Level	[edit forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output], [edit forwarding-options sampling family (inet   inet6   mpls) output]
Release Information	Statement introduced before Junos OS Release 7.4. version9 statement introduced in Junos OS Release 8.3.
Description	<p>Collect an aggregate of sampled flows and send the aggregate to a specified host system that runs the collection utility cfdcollect. Specify a host system to collect sampled flows using the version 9 format.</p> <p>You can configure up to one version 5 and one version 8 flow format at the [edit forwarding-options sampling family (inet   inet6   mpls) output flow-server <i>hostname</i>] hierarchy level. For the same configuration, you can specify only either version 9 flow record formats or formats using versions 5 and 8, not both types of formats.</p>
Options	<p><b>hostname</b>—The IP address—IPv4 or IPv6—or identifier of the host system (the workstation either running the cflowd utility or collecting traffic flows using version 9).</p> <p>You can configure only one host system for version 9.</p>



**NOTE:** IPv6 configuration for flow-server is supported only in Junos OS Release 12.3 and later.

Note that when you configure an IPv6 address for the flow-server statement, you must also configure an IPv6 address for the inline-jflow source-address statement at the [edit forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls) output] hierarchy level.

The remaining statements are explained separately.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li></ul>

---

## forwarding-options

---

<b>Syntax</b>	forwarding-options { ... }
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure traffic forwarding.  The statements that apply to services interfaces are explained separately. For other statements, see the <i>Routing Policy Feature Guide for Routing Devices</i> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li></ul>

---

## inline-jflow

---

<b>Syntax</b>	inline-jflow { <a href="#">source-address</a> <i>address</i> ; <a href="#">flow-export-rate</a> <i>rate</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options</a> <a href="#">sampling instance</a> <i>instance-name</i> <a href="#">family</a> inet <a href="#">output</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify inline flow monitoring for traffic from the designated address.
<b>Options</b>	<i>address</i> —Source IP address.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Inline Sampling on page 1176</a></li></ul>

## input

---

See the following sections:

- [input \(Port Mirroring\) on page 1244](#)
- [input \(Sampling\) on page 1245](#)

### input (Port Mirroring)

Syntax	<pre>input {   maximum-packet-length <i>bytes</i>   rate <i>number</i>;   run-length <i>number</i>; }</pre>
Hierarchy Level	<pre>[edit forwarding-options port-mirroring], [edit forwarding-options port-mirroring instance <i>instance-name</i>] [edit forwarding-options port-mirroring family (inet   inet6)]</pre>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure port mirroring on a logical interface.</p> <p>The statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port Mirroring on page 1186</a></li></ul>

## input (Sampling)

<b>Syntax</b>	<pre>input {   max-packets-per-second <i>number</i>;   rate <i>number</i>;   run-length <i>number</i>;   maximum-packet-length <i>bytes</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options sampling</a> ], [edit <a href="#">forwarding-options sampling instance</a> <i>instance-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure traffic sampling on a logical interface.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li></ul>

## input-interface-index

---

<b>Syntax</b>	<pre>input-interface-index <i>number</i>;</pre>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options monitoring name</a> <a href="#">output interface</a> <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify a value for the input interface index that overrides the default supplied by SNMP.
<b>Options</b>	<i>number</i> —Input interface index value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li></ul>

## instance

---

See the following sections:

- [instance \(Port Mirroring\) on page 1246](#)
- [instance \(Sampling\) on page 1247](#)

### instance (Port Mirroring)

**Syntax**     `instance instance-name {  
              disable;  
              input {  
                  rate number;  
                  maximum-packet-length bytes  
              }  
              family (any | inet | inet6 | vpls) {  
                  output {  
                      (next-hop-group group-name | interface interface-name);  
                  }  
              }  
              }`

**Hierarchy Level**     [edit [forwarding-options](#) port-mirroring]

**Release Information**     Statement introduced in Junos OS Release 9.6.

**Description**     Configure a port-mirroring instance.

The remaining statements are explained separately.

**Usage Guidelines**     See “[Sampling Instance Configuration](#)” on page 1175.

**Required Privilege Level**     interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

## instance (Sampling)

```
Syntax  instance instance-name {
        disable;
        input {
            rate number;
            run-length number;
            max-packets-per-second number;
            maximum-packet-length bytes;
        }
        family (inet | inet6 | mpls) {
            disable;
            output {
                aggregate-export-interval seconds;
                flow-active-timeout seconds;
                flow-inactive-timeout seconds;
                extension-service service-name;
                flow-server hostname {
                    aggregation {
                        autonomous-system;
                        destination-prefix;
                        protocol-port;
                        source-destination-prefix {
                            caida-compliant;
                        }
                        source-prefix;
                    }
                    autonomous-system-type (origin | peer);
                    (local-dump | no-local-dump);
                    port port-number;
                    source-address address;
                    version format;
                    version9 {
                        template template-name;
                    }
                }
            }
            interface interface-name {
                engine-id number;
                engine-type number;
                source-address address;
            }
            inline-jflow {
                source-address address;
                flow-export-rate rate;
            }
        }
    }
```

**Hierarchy Level** [edit [forwarding-options sampling](#)]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Configure a sampling instance.

The remaining statements are explained separately.

<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Sampling Instance Configuration on page 1175</a></li></ul>

## interface

---

See the following sections:

- [interface \(Accounting or Sampling\) on page 1249](#)
- [interface \(Monitoring\) on page 1250](#)
- [interface \(Port Mirroring\) on page 1250](#)

### interface (Accounting or Sampling)

<b>Syntax</b>	<pre>interface <i>interface-name</i> {     <b>engine-id</b> <i>number</i>;     <b>engine-type</b> <i>number</i>;     <b>source-address</b> <i>address</i>; }</pre>
<b>Hierarchy Level</b>	[edit <b>forwarding-options accounting</b> <i>name</i> <b>output</b> ], [edit <b>forwarding-options sampling family</b> (inet   inet6   mpls) <b>output</b> ], [edit <b>forwarding-options sampling instance</b> <i>instance-name</i> <b>family</b> (inet   inet6   mpls) <b>output</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the output interface for monitored traffic.
<b>Options</b>	<p><b><i>interface-name</i></b>—Name of the interface.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p><b>interface</b>—To view this statement in the configuration.</p> <p><b>interface-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Discard Accounting on page 1202</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> </ul>

## interface (Monitoring)

Syntax	<pre>interface <i>interface-name</i> {     <i>engine-id</i> <i>number</i>;     <i>engine-type</i> <i>number</i>;     <i>input-interface-index</i> <i>number</i>;     <i>output-interface-index</i> <i>number</i>;     <i>source-address</i> <i>address</i>; }</pre>
Hierarchy Level	[edit <b>forwarding-options monitoring</b> <i>name</i> <b>family</b> inet <b>output</b> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the output interface for monitored traffic.
Options	<i>interface-name</i> —Name of the interface.  The remaining statements are explained separately.
Usage Guidelines	See “ <a href="#">Configuring Flow Monitoring</a> ” on page 1144.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## interface (Port Mirroring)

Syntax	<pre>interface <i>interface-name</i> {     <i>next-hop</i> <i>address</i>; }</pre>
Hierarchy Level	[edit <b>forwarding-options port-mirroring</b> <b>family</b> (inet   inet6) <b>output</b> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the output interface for sending copies of packets elsewhere to be analyzed.
Options	<i>interface-name</i> —Name of the interface.  The remaining statements are explained separately.
Usage Guidelines	See “ <a href="#">Configuring Port Mirroring</a> ” on page 1186.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## interfaces

---

<b>Syntax</b>	interfaces { ... }
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure interfaces on the router.
<b>Default</b>	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
<b>Usage Guidelines</b>	See the <i>Junos OS Network Interfaces Library for Routing Devices</i> for general information.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## ipv4-template

---

<b>Syntax</b>	ipv4-template;
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring version9 template template-name</a> ] [edit <a href="#">services flow-monitoringversion-ipfix template template-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. Support at the [edit <a href="#">services flow-monitoring version-ipfix template template-name</a> ] hierarchy level added in Junos OS Release 10.2.
<b>Description</b>	Specify that the flow aggregation version 9 template is used only for IPv4 records.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156</a></li> </ul>

## ipv6-template

---

<b>Syntax</b>	ipv6-template;
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring version9 template <i>template-name</i></a> ] [edit <a href="#">services flow-monitoringversion-ipfix template <i>template-name</i></a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4. Support at the [edit <a href="#">services flow-monitoring version-ipfix template <i>template-name</i></a> ] hierarchy level added in Junos OS Release 10.2.
<b>Description</b>	Specify that the flow aggregation version 9 template is used only for IPv6 records.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156</a></li></ul>

## label-position

---

<b>Syntax</b>	label-position [ <i>positions</i> ];
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring version9 template <i>template-name</i> mpls-ipv4-template</a> ], [edit <a href="#">services flow-monitoring version9 template <i>template-name</i> mpls-template</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	Specify positions for up to three labels in the active flow monitoring version 9 template.
<b>Default</b>	[1 2 3]
<b>Options</b>	<i>positions</i> —Numbered positions for the labels.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156</a></li></ul>

## local-dump

<b>Syntax</b>	(local-dump   no-local-dump);
<b>Hierarchy Level</b>	[edit forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output flow-server <i>hostname</i> ], [edit forwarding-options sampling family (inet   inet6   mpls) output flow-server <i>hostname</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Enable collection of cflowd records in a log file.
<b>Options</b>	<b>no-local-dump</b> —Do not dump cflowd records to a log file before exporting.  <b>local-dump</b> —Dump cflowd records to a log file before exporting.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Enabling Flow Aggregation on page 1151</a></li> </ul>

## match

<b>Syntax</b>	match <i>expression</i> ;
<b>Hierarchy Level</b>	[edit forwarding-options port-mirroring traceoptions <i>file</i> ], [edit forwarding-options sampling traceoptions <i>file</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Regular expression for lines to be logged for tracing.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Port Mirroring on page 1186</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> </ul>

## maximum-packet-length

---

<b>Syntax</b>	<code>maximum-packet-length bytes;</code>
<b>Hierarchy Level</b>	[edit forwarding-options port-mirroring input], [edit forwarding-options port-mirroring instance <i>instance-name</i> input], [edit forwarding-options <a href="#">sampling input</a> ], [edit <a href="#">forwarding-options sampling instance</a> <i>instance-name</i> input]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
<b>Description</b>	Set the maximum length of the packet used for port mirroring or traffic sampling. Packets with lengths greater than the specified maximum are truncated.




**NOTE:** The `maximum-packet-length` statement is not supported on MX80 routers.



**NOTE:** For MX-Series devices with Modular Port Interface Concentrators (MPCs), when `maximum-packet-length` (clip length) is configured for port-mirrored packets and the mirror-destination interface is a next-hop-group, the clip length would be effective only for the first member interface of the next-hop-group. The mirrored packet copy sent to the rest of the interfaces would not be clipped.

<b>Options</b>	<code>bytes</code> —Maximum length (in bytes) of the mirrored packet or the sampled packet. <b>Range:</b> 0 through 9216 <b>Default:</b> 0  For MX-Series devices with Modular Port Concentrators (MPCs), port-mirrored or sampled packets can be truncated (or clipped) to any length in the range of 1 to 255 bytes. Only 1 to 255 are valid values for packet truncation on these devices. For other devices, the range is from 0 to 9216. A <code>maximum-packet-length</code> value of zero represents that truncation is disabled, and the entire packet is mirrored or sampled.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port Mirroring</a></li><li>• <a href="#">Configuring Traffic Sampling</a></li></ul>

## max-packets-per-second

<b>Syntax</b>	<code>max-packets-per-second <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options sampling input</a> ], [edit <a href="#">forwarding-options sampling instance <i>instance-name</i> input</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the traffic threshold that must be exceeded before packets are dropped. A value of 0 instructs the Packet Forwarding Engine not to sample any traffic.
<div>  <p><b>NOTE:</b> When you configure active monitoring and specify a Monitoring Services, Adaptive Services, or Multiservices PIC in the output statement, the <code>max-packets-per-second</code> value is ignored.</p> </div>	
<b>Options</b>	<p><i>number</i>—Maximum number of packets per second.</p> <p><b>Range:</b> 0 through 65,535</p> <p><b>Default:</b> 1000</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> </ul>

## monitoring

---

```
Syntax  monitoring name {  
        family inet {  
            output {  
                cflowd hostname port-number;  
                export-format cflowd-version-5;  
                flow-active-timeout seconds;  
                flow-export-destination {  
                    (cflowd-collector | collector-pic);  
                }  
                flow-inactive-timeout seconds;  
                interface interface-name {  
                    number;  
                    engine-type number;  
                    input-interface-index number;  
                    output-interface-index number;  
                    source-address address;  
                }  
            }  
        }  
    }
```

**Hierarchy Level**    [edit [forwarding-options](#)]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Specify the flow monitoring instance name and properties.

The statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                 interface-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring Flow Monitoring on page 1144](#)

## mpls-ipv4-template

---

<b>Syntax</b>	<code>mpls-ipv4-template {     label-position [ <i>positions</i> ]; }</code>
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring version9 template <i>template-name</i></a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	Specify the flow aggregation version 9 properties for templates that combine IPv4 and MPLS records. The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156</a></li> </ul>

## mpls-template

---

<b>Syntax</b>	<code>mpls-template {     label-position [ <i>positions</i> ]; }</code>
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring version9 template <i>template-name</i></a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	Specify the flow aggregation version 9 properties for templates used only for MPLS records. The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156</a></li> </ul>

## multiservice-options

---

<b>Syntax</b>	<pre>multiservice-options {   (core-dump   no-core-dump);   (syslog   no-syslog);   flow-control-options {     down-on-flow-control;     dump-on-flow-control;     reset-on-flow-control;   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>mo-fpc/pic/port</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For flow-monitoring interfaces only, configure multiservice-specific interface properties.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li></ul>

## next-hop (Forwarding Options)

---

<b>Syntax</b>	<pre>next-hop <i>address</i>;</pre>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options</a> <a href="#">port-mirroring</a> <a href="#">family</a> (inet   inet6) <a href="#">output</a> <a href="#">interface</a> <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the next-hop address for sending copies of packets to an analyzer.
<b>Options</b>	<b><i>address</i></b> —IP address of the next-hop router.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port Mirroring on page 1186</a></li></ul>

## next-hop-group

See the following sections:

- [next-hop-group \(Forwarding Options\) on page 1259](#)
- [next-hop-group \(Port Mirroring\) on page 1260](#)

### next-hop-group (Forwarding Options)

**Syntax**    `next-hop-group group-name {  
                  interface interface-name {  
                    next-hop address;  
                  }  
                  }`

**Hierarchy Level**    [edit [forwarding-options](#)]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Specify the next-hop address for sending copies of packets to an analyzer.

It is implicitly assumed that a subgroup is up only if more than one interface in the subgroup is up.

**Options**    ***address***—IP address of the next-hop router. Each next-hop group supports up to 16 next-hop addresses. Up to 30 next-hop groups are supported. Each next-hop group must have at least two next-hop addresses.

***group-name***—Name of next-hop group. Up to 30 next-hop groups are supported for the router. Each next-hop group is expected to have at least two next-hop addresses.

***interface-name***—Name of interface used to reach the next-hop destination.

**Required Privilege Level**    interface—To view this statement in the configuration.  
   interface-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring Port Mirroring on page 1186](#)

## next-hop-group (Port Mirroring)

<b>Syntax</b>	<code>next-hop-group <i>group-name</i>;</code>
<b>Hierarchy Level</b>	[edit forwarding-options port-mirroring family (inet   vpls) output], [edit forwarding-options port-mirroring instance <i>instance-name</i> family (inet   vpls) output]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Specify the next-hop address for sending copies of packets to an analyzer. This configuration enables multipacket port mirroring on MX Series routers and EX Series switches without the use of a Tunnel PIC.</p> <p>The commit operation fails when a next-hop group has only one interface configured. It is implicitly assumed that a subgroup is up only if more than one interface in the subgroup is up.</p>
<b>Options</b>	<i>group-name</i> —Name of next-hop group.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Port Mirroring with Next-Hop Groups on page 1188</a></li></ul>

---

## no-core-dump

See [core-dump](#)

---

## no-filter-check

<b>Syntax</b>	<code>no-filter-check;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options port-mirroring family</a> (inet   inet6) <a href="#">output</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Disable filter checking on the port-mirroring interface.</p> <p>This statement is required when you send port-mirrored traffic to a Tunnel PIC that has a filter applied to it.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port Mirroring on page 1186</a></li></ul>

---

## no-local-dump

See [local-dump](#)

## no-remote-trace (Trace Options)

---

<b>Syntax</b>	no-remote-trace;
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options port-mirroring traceoptions</a> ], [edit <a href="#">forwarding-options sampling traceoptions</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Disable remote tracing.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Tracing Traffic Sampling Operations on page 1140</a></li></ul>

## no-stamp

---

See [stamp](#)

## no-syslog

---

See [syslog](#)

## no-world-readable

---

See [world-readable](#)

## observation-domain-id

---

<b>Syntax</b>	<code>observation-domain-id <i>domain-id</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring</a> <a href="#">version-ipfix</a> <a href="#">template</a> <i>template-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	<p>For IPFIX flows, an identifier of an Observation Domain is locally unique to an exporting process of the templates. The export process uses the Observation Domain ID to uniquely identify to the collection process in which the flows were metered. We recommend that you configure this ID to be unique for each IPFIX flow. A value of 0 indicates that no specific Observation Domain is identified by this information element. Typically, this attribute is used to limit the scope of other information elements. If the observation domain is not unique, the collector cannot uniquely identify an IPFIX device.</p> <p>If you configure the same Observation Domain ID for different template types, such as for IPv4 and IPv6, it does not impact flow monitoring because the actual or the base observation domain ID is transmitted in the flow. The actual observation domain ID is derived from the value you configure and also in conjunction with other parameters such as the slot number, lookup chip (LU) instance, Packet Forwarding Engine instance. Such a method of computation of the observation domain ID ensures that this ID is not the same for two IPFIX devices.</p>
<b>Options</b>	<p><b><i>domain-id</i></b>—Specify a unique identifier for the observation domain for IPFIX flows.</p> <p><b>Range:</b> 0 through 255</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows on page 1172</a></li><li>• <a href="#">Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 1167</a></li></ul>

## option-refresh-rate

---

<b>Syntax</b>	<code>option-refresh-rate packets <i>packets</i> seconds <i>seconds</i>;</code>
<b>Hierarchy Level</b>	<code>[edit <a href="#">services flow-monitoring version9</a>],</code> <code>[edit <a href="#">services flow-monitoring version9 template <i>template-name</i></a>]</code> <code>[edit <a href="#">services flow-monitoringversion-ipfix template <i>template-name</i></a>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. Support at the <code>[edit <a href="#">services flow-monitoring version-ipfix template <i>template-name</i></a>]</code> hierarchy level added in Junos OS Release 10.2.
<b>Description</b>	Specify the refresh rate, in either packets or seconds.
<b>Options</b>	<b><i>packets</i></b> —Refresh rate, in number of packets. <b>Range:</b> 1 through 480,000 <b>Default:</b> 4800  <b><i>seconds</i></b> —Refresh rate, in number of seconds. <b>Range:</b> 10 through 600 <b>Default:</b> 600
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156</a></li></ul>

## options-template-id

---

<b>Syntax</b>	<code>options-template-id <i>id</i>;</code>
<b>Hierarchy Level</b>	<code>[edit <a href="#">services flow-monitoring version9 template</a> <i>template-name</i>]</code> <code>[edit <a href="#">services flow-monitoringversion-ipfix template</a> <i>template-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Define a unique options template ID to be used for flow aggregation of version 9 and IPFIX flows. If you do not configure values for the template ID and options template ID, default values are assumed for these IDs, which are different for the various address families. If you configure the same template ID or options template ID value for different address families, such a setting is not processed properly and might cause unexpected behavior. For example, if you configure the same template ID value for both IPv4 and IPv6, the collector validates the export data based on the template ID value that it last receives. In this case, if IPv6 is configured after IPv4, the value is effective for IPv6 and the default value is used for IPv4.
<b>Options</b>	<i>id</i> —Specify a unique identifier for the options template to be used for version 9 or IPFIX flows. <b>Range:</b> 1024 through 65535
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows on page 1172</a></li><li>• <a href="#">Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 1167</a></li></ul>

## output

See the following sections:

- [output \(Accounting\) on page 1265](#)
- [output \(Monitoring\) on page 1266](#)
- [output \(Port Mirroring\) on page 1267](#)
- [output \(Sampling\) on page 1268](#)

### output (Accounting)

**Syntax**

```
output {
  aggregate-export-interval seconds;
  cflowd hostname {
    aggregation {
      autonomous-system;
      destination-prefix;
      protocol-port;
      source-destination-prefix {
        caida-compliant;
      }
      source-prefix;
    }
    autonomous-system-type (origin | peer);
    (local-dump | no-local-dump);
    port port-number;
    source-address address;
    version format;
  }
  flow-active-timeout seconds;
  flow-inactive-timeout seconds;
  interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
  }
}
```

**Hierarchy Level** [edit [forwarding-options accounting name](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure cflowd, output interfaces, and flow properties.

The statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Discard Accounting on page 1202](#)

## output (Monitoring)

**Syntax**

```
output {  
  cflowd hostname port port-number;  
  export-format format;  
  flow-active-timeout seconds;  
  flow-export-destination {  
    (cflowd-collector | collector-pic);  
  }  
  flow-inactive-timeout seconds;  
  interface interface-name {  
    engine-id number;  
    engine-type number;  
    input-interface-index number;  
    output-interface-index number;  
    source-address address;  
  }  
}
```

**Hierarchy Level** [edit [forwarding-options monitoring name](#) family inet]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure cflowd, output interfaces, and flow properties.

The statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Flow Monitoring on page 1144](#)

## output (Port Mirroring)

Syntax	<pre>output {   interface <i>interface-name</i> {     next-hop <i>address</i>;   }   no-filter-check; }</pre>
Hierarchy Level	[edit <a href="#">forwarding-options port-mirroring family</a> (inet   inet6)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure output interfaces and flow properties.</p> <p>The statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port Mirroring on page 1186</a></li></ul>

## output (Sampling)

**Syntax**

```
output {  
  aggregate-export-interval seconds;  
  flow-active-timeout seconds;  
  flow-inactive-timeout seconds;  
  extension-service service-name;  
  flow-server hostname {  
    aggregation {  
      autonomous-system;  
      destination-prefix;  
      protocol-port;  
      source-destination-prefix {  
        caida-compliant;  
      }  
      source-prefix;  
    }  
    autonomous-system-type (origin | peer);  
    (local-dump | no-local-dump);  
    port port-number;  
    source-address address;  
    version format;  
    version9 {  
      template template-name;  
    }  
  }  
  interface interface-name {  
    engine-id number;  
    engine-type number;  
    source-address address;  
  }  
  file {  
    disable;  
    filename filename;  
    files number;  
    size bytes;  
    (stamp | no-stamp);  
    (world-readable | no-world-readable);  
  }  
  inline-jflow {  
    source-address address;  
    flow-export-rate rate;  
  }  
}
```

**Hierarchy Level** [edit **forwarding-options sampling instance** *instance-name* **family** (*inet* | *inet6* | *mpls*)],  
[edit **forwarding-options sampling family** (*inet* | *inet6* | *mpls*)]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure cflowd or flow monitoring, output files and interfaces, and flow properties.  
  
The statements are explained separately.



**NOTE:** The `inline-jflow` statement is valid only under the `[edit forwarding-options sampling instance instance-name family inet output]` hierarchy level. The `file` statement is valid only under the `[edit forwarding-options sampling family inet output]` hierarchy level.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation** • [Configuring Traffic Sampling on page 1134](#)

## output-interface-index

**Syntax** `output-interface-index number;`

**Hierarchy Level** `[edit forwarding-options monitoring name output interface interface-name]`

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Specify a value for the output interface index that overrides the default supplied by SNMP.



**NOTE:** On J Series routers, `cflowd` sampling in the input direction of an interface reports the output interface index as 0.

**Options** *number*—Output interface index value.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation** • [Configuring Flow Monitoring on page 1144](#)

## passive-monitor-mode

---

<b>Syntax</b>	<code>passive-monitor-mode;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Asynchronous Transfer Mode (ATM), SONET/SDH, Fast Ethernet, and Gigabit Ethernet interfaces only, monitor packet flows from another router. If you include this statement in the configuration, the SONET/SDH interface does not send keepalives or alarms, and does not participate actively on the network.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Enabling Passive Flow Monitoring on page 1203</a></li><li>• <a href="#">multiservice-options on page 1258</a></li></ul>

## pop-all-labels

---

<b>Syntax</b>	pop-all-labels { required-depth <i>number</i> ; }
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> atm-options mpls], [edit interfaces <i>interface-name</i> fastether-options mpls], [edit interfaces <i>interface-name</i> gigether-options mpls], [edit interfaces <i>interface-name</i> sonet-options mpls]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For passive monitoring on ATM, SONET/SDH, Fast Ethernet, and Gigabit Ethernet interfaces only, removes up to two MPLS labels from incoming IP packets. For passive monitoring on T Series devices, removes up to five MPLS labels from incoming IP packets.</p> <p>This statement has no effect on IP packets with more than two MPLS labels, or IP packets with more than five MPLS labels on T Series devices. Packets with MPLS labels cannot be processed by the monitoring PIC; if packets with MPLS labels are forwarded to the monitoring PIC, they are discarded.</p> <p>The remaining statement is explained separately.</p>
<b>Default</b>	If you omit this statement, the MPLS labels are not removed, and the packet is not processed by the monitoring PIC.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Passive Flow Monitoring for MPLS Encapsulated Packets on page 1205</a></li> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li> </ul>

## port

---

<b>Syntax</b>	<code>port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options accounting</a> <i>name</i> <a href="#">output cflowd</a> <i>hostname</i> ], [edit <a href="#">forwarding-options monitoring</a> <i>name</i> <a href="#">family</a> <a href="#">inet</a> <a href="#">output cflowd</a> <i>hostname</i> ], [edit <a href="#">forwarding-options sampling instance</a> <i>instance-name</i> <a href="#">family</a> ( <a href="#">inet</a>   <a href="#">inet6</a>   <a href="#">mpls</a> ) <a href="#">output</a> <a href="#">flow-server</a> <i>hostname</i> ], [edit <a href="#">forwarding-options sampling family</a> ( <a href="#">inet</a>   <a href="#">inet6</a>   <a href="#">mpls</a> ) <a href="#">output flow-server</a> <i>hostname</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the User Datagram Protocol (UDP) port number on the cflowd host system or flow server.
<b>Options</b>	<i>port-number</i> —Any valid UDP port number on the host system.
<b>Required Privilege Level</b>	<a href="#">interface</a> —To view this statement in the configuration. <a href="#">interface-control</a> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Enabling Flow Aggregation on page 1151</a></li></ul>

## port-mirroring

```
Syntax  port-mirroring {
        input {
            maximum-packet-length bytes
            rate rate;
            run-length number;
        }
        family any {
            output {
                (next-hop-group group-name | interface interface-name);
            }
        }
        family inet {
            output {
                interface interface-name {
                    next-hop address;
                }
                no-filter-check;
            }
        }
        instance instance-name {
            input {
                rate rate;
                maximum-packet-length number;
            }
            family any {
                output {
                    (next-hop-group group-name | interface interface-name);
                }
            }
            family inet {
                output {
                    next-hop-group group-name;
                }
            }
        }
        traceoptions {
            file filename <files number> <size bytes> <world-readable | no-world-readable>;
        }
    }
```

Hierarchy Level [edit [forwarding-options](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement **family any** introduced in Junos OS Release 13.2.

**Description** Specify the input, output, and traceoptions properties for sending copies of packets to an analyzer.



**NOTE:** Option **run-length** is not supported on MX Series routers with MPCs.

The statements are explained separately.

<b>Usage Guidelines</b>	See <a href="#">“Configuring Port Mirroring” on page 1186</a> .
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.

---

## rate (Forwarding Options)

---

<b>Syntax</b>	<code>rate <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options port-mirroring input</a> ], [edit <a href="#">forwarding-options sampling input</a> ], [edit <a href="#">forwarding-options sampling instance <i>instance-name</i> input</a> ], [edit <a href="#">forwarding-options port-mirroring family (inet inet6) input</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
<b>Description</b>	Set a ratio of the number of packets to be sampled. For example, if you specify a rate of 10, every tenth packet (1 packet out of 10) is sampled.
<b>Options</b>	<i>number</i> —Denominator of the ratio. <b>Range:</b> 1 through 65,535
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Port Mirroring</a></li><li>• <a href="#">Configuring Traffic Sampling</a></li></ul>

---

## receive-options-packets

---

<b>Syntax</b>	<code>receive-options-packets;</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	When you enable passive monitoring, this statement is required for conformity with cflowd records structure.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Enabling Passive Flow Monitoring on page 1203</a></li></ul>

## receive-ttl-exceeded

<b>Syntax</b>	receive-ttl-exceeded;
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> <a href="#">unit</a> <i>logical-unit-number</i> <a href="#">family</a> inet]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	When you enable passive monitoring, this statement is required for conformity with cflowd records structure.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Enabling Passive Flow Monitoring on page 1203</a></li> </ul>

## required-depth

<b>Syntax</b>	required-depth <i>number</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> atm-options mpls <a href="#">pop-all-labels</a> ], [edit <a href="#">interfaces</a> <i>interface-name</i> fastether-options mpls <a href="#">pop-all-labels</a> ], [edit <a href="#">interfaces</a> <i>interface-name</i> gigether-options mpls <a href="#">pop-all-labels</a> ], [edit <a href="#">interfaces</a> <i>interface-name</i> sonet-options mpls <a href="#">pop-all-labels</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For passive monitoring on ATM, SONET/SDH, Fast Ethernet, and Gigabit Ethernet interfaces only, specify the number of MPLS labels an incoming packet must have for the <b>pop-all-labels</b> statement to take effect.</p> <p>If you include the <b>required-depth 1</b> statement, the <b>pop-all-labels</b> statement takes effect for incoming packets with one label only. If you include the <b>required-depth 2</b> statement, the <b>pop-all-labels</b> statement takes effect for incoming packets with two labels only.</p>
<b>Options</b>	<p><b>number</b>—Number of MPLS labels on incoming IP packets.</p> <p><b>Range:</b> 1 through 2 labels.</p> <p><b>Default:</b> If you omit this statement, the <b>pop-all-labels</b> statement takes effect for incoming packets with one or two labels. The default is equivalent to including the <b>required-depth [ 1 2 ]</b> statement.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Passive Flow Monitoring for MPLS Encapsulated Packets on page 1205</a></li> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li> </ul>

## run-length

---

<b>Syntax</b>	<code>run-length <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options port-mirroring input</a> ], [edit forwarding-options port-mirroring instance <i>port-mirroring-instance-name</i> input], [edit <a href="#">forwarding-options port-mirroring family (inet inet6) input</a> ], [edit <a href="#">forwarding-options sampling input</a> ], [edit <a href="#">forwarding-options sampling instance instance-name input</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
<b>Description</b>	Set the number of samples following the initial trigger event. The configuration enables you to sample packets following those already being sampled.
<b>Options</b>	<i>number</i> —Number of samples. <b>Range:</b> 0 through 20 <b>Default:</b> 0
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying Filters to Forwarding Tables</a></li><li>• <a href="#">Configuring Port Mirroring on page 1186</a></li><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li></ul>

## sample-once

---

<b>Syntax</b>	<code>sample-once;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options sampling</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Sample traffic for active monitoring only once.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li></ul>

## sampling

---

See the following sections:

- [sampling \(Forwarding Options\) on page 1278](#)
- [sampling \(Interfaces\) on page 1280](#)

## sampling (Forwarding Options)

```
Syntax  sampling {
        disable;
        sample-once;
        family (inet | inet6 | mpls) {
            disable;
            output {
                aggregate-export-interval seconds;
                extension-service service-name;
                file {
                    disable;
                    filename filename;
                    files number;
                    size bytes;
                    (stamp | no-stamp);
                    (world-readable | no-world-readable);
                }
                flow-active-timeout seconds;
                flow-inactive-timeout seconds;
                flow-server hostname {
                    aggregation {
                        autonomous-system;
                        destination-prefix;
                        protocol-port;
                        source-destination-prefix {
                            caida-compliant;
                        }
                        source-prefix;
                    }
                    autonomous-system-type (origin | peer);
                    (local-dump | no-local-dump);
                    port port-number;
                    source-address address;
                    version format;
                    version9 {
                        template template-name;
                    }
                }
            }
            interface interface-name {
                engine-id number;
                engine-type number;
                source-address address;
            }
        }
    }
    input {
        max-packets-per-second number;
        maximum-packet-length bytes;
        rate number;
        run-length number;
    }
    instance instance-name {
        disable;
        family (inet | inet6 | mpls) {
```

```

disable;
output {
    aggregate-export-interval seconds;
    extension-service service-name;
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    flow-server hostname {
        aggregation {
            autonomous-system;
            destination-prefix;
            protocol-port;
            source-destination-prefix {
                caida-compliant;
            }
            source-prefix;
        }
        autonomous-system-type (origin | peer);
        (local-dump | no-local-dump);
        port port-number;
        source-address address;
        version format;
        version-ipfix {
            template template-name;
        }
        version9 {
            template template-name;
        }
    }
    inline-jflow {
        source-address address;
        flow-export-rate rate;
    }
    interface interface-name {
        engine-id number;
        engine-type number;
        source-address address;
    }
}
input {
    max-packets-per-second number;
    maximum-packet-length bytes;
    rate number;
    run-length number;
}
pre-rewrite-tos;
traceoptions {
    no-remote-trace;
    file filename <files number> <size bytes> <match expression> <world-readable |
    no-world-readable>;
}
}

```

Hierarchy Level    [edit [forwarding-options](#)]

<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
<b>Description</b>	Configure traffic sampling.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li><li>• <i>Applying Filters to Forwarding Tables</i></li><li>• <i>Configuring Active Flow Monitoring Using Version 9</i></li><li>• <i>Configuring Flow Aggregation (cflowd)</i></li><li>• <i>Configuring Port Mirroring</i></li><li>• <i>Tracing Traffic-Sampling Operations</i></li></ul>

## sampling (Interfaces)

<b>Syntax</b>	sampling <i>direction</i> ;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the direction of traffic to be sampled.
<b>Options</b>	<p><i>direction</i> can be one of the following:</p> <p><b>input</b>—Configure at least one expected ingress point.</p> <p><b>output</b>—Configure at least one expected egress point.</p> <p><b>input output</b>—On a single interface, configure at least one expected ingress point and one expect egress point.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Junos OS Services Interfaces Library for Routing Devices</i></li><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li></ul>

## services

---

<b>Syntax</b>	<code>services { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure router services.  The underlying statements are explained separately.
<b>Usage Guidelines</b>	See <a href="#">“Configuring Flow Aggregation to Use Version 9 Flow Templates”</a> on page 1156.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## size

---

<b>Syntax</b>	<code>size bytes;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options port-mirroring traceoptions file</a> ], [edit <a href="#">forwarding-options sampling family (inet   inet6   mpls) output file</a> ], [edit <a href="#">forwarding-options sampling traceoptions file</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the maximum size of each file containing sample or log data. The file size is limited by the number of files to be created and the available hard disk space.  When a traffic sampling file named <b>sampling-file</b> reaches the maximum size, it is renamed <b>sampling-file.0</b> . When the <b>sampling-file</b> again reaches its maximum size, <b>sampling-file.0</b> is renamed <b>sampling-file.1</b> and <b>sampling-file</b> is renamed <b>sampling-file.0</b> . This renaming scheme continues until the maximum number of traffic sampling files is reached. Then the oldest traffic sampling file is overwritten.
<b>Options</b>	<b>bytes</b> —Maximum size of each traffic sampling file or trace log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). <b>Syntax:</b> <i>xk</i> to specify KB, <i>xm</i> to specify MB, or <i>xg</i> to specify GB <b>Range:</b> 10 KB through the maximum file size supported on your router <b>Default:</b> 1 MB for sampling data; 128 KB for log information
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Port Mirroring</a> on page 1186</li> <li>• <a href="#">Configuring Traffic Sampling</a> on page 1134</li> </ul>

## source-address (Forwarding Options)

---

<b>Syntax</b>	<code>source-address <i>address</i>;</code>
<b>Hierarchy Level</b>	<code>[edit forwarding-options accounting <i>name</i> output interface <i>interface-name</i>],</code> <code>[edit forwarding-options monitoring <i>name</i> family <i>family</i> inet output interface <i>interface-name</i>],</code> <code>[edit forwarding-options sampling instance <i>instance-name</i> family (inet   inet6   mpls) output</code> <code>interface <i>interface-name</i>],</code> <code>[edit forwarding-options sampling family (inet   inet6   mpls) output interface <i>interface-name</i>],</code> <code>[edit forwarding-options sampling instance <i>instance-name</i> family inet output inline-jflow]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the source address for monitored packets.
<b>Options</b>	<i>address</i> —Interface source address.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Discard Accounting on page 1202</a></li><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li></ul>

## source-id

---

<b>Syntax</b>	<code>source-id <i>source-id</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services flow-monitoring version9 template <i>template-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	For version 9 flows, a 32-bit value that identifies the Exporter Observation Domain is called the source ID. NetFlow collectors use the combination of the source IP address and the source ID field to separate different export streams originating from the same exporter.
<b>Options</b>	<i>source-id</i> —Specify a unique identifier for the source for version 9 flows. <b>Range:</b> 0 through 255
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows on page 1172</a></li><li>• <a href="#">Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 1167</a></li></ul>

## stamp

---

<b>Syntax</b>	(stamp   no-stamp);
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options sampling family</a> (inet   inet6   mpls) <a href="#">output file</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Include a timestamp with each line in the output file.
<b>Options</b>	<b>no-stamp</b> —Do not include timestamps. This is the default. <b>stamp</b> —Include a timestamp with each line of packet sampling information. <b>Default:</b> No timestamp is included.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li></ul>

## syslog

---

<b>Syntax</b>	(syslog   no-syslog);
<b>Hierarchy Level</b>	[edit <a href="#">interfaces mo-fpc/pic/port multiservice-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	System logging is enabled by default. The system log information of the Monitoring Services PIC is passed to the kernel for logging in the <b>/var/log</b> directory. <ul style="list-style-type: none"><li>• <b>syslog</b>—Enable PIC system logging.</li><li>• <b>no-syslog</b>—Disable PIC system logging.</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li></ul>

## template

---

See the following sections:

- [template \(Forwarding Options\) on page 1284](#)
- [template \(Services\) on page 1285](#)

### template (Forwarding Options)

<b>Syntax</b>	<code>template <i>template-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options sampling instance</a> <i>instance-name</i> <a href="#">family</a> (inet   inet6   mpls) <a href="#">output flow-server</a> <i>hostname</i> <a href="#">version9</a> ], [edit <a href="#">forwarding-options sampling family</a> (inet   inet6   mpls) <a href="#">output flow-server</a> <i>hostname</i> <a href="#">version9</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	Specify flow monitoring version 9 template to be used for output of sampling records.
<b>Options</b>	<i>template-name</i> —Name of the version 9 template.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156</a></li></ul>

## template (Services)

<b>Syntax</b>	<pre> template <i>template-name</i> {   flow-active-timeout <i>seconds</i>;   flow-inactive-timeout <i>seconds</i>;   ipv4-template;   ipv6-template;   mpls-template {     label-position [ <i>positions</i> ];   }   mpls-ipv4-template {     label-position [ <i>positions</i> ];   }   peer-as-billing-template;   option-refresh-rate packets <i>packets</i> seconds <i>seconds</i>;   template-refresh-rate packets <i>packets</i> seconds <i>seconds</i>; } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring version9</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	Specify the flow aggregation version 9 template properties. The remaining statements are explained separately.
<b>Options</b>	<i>template-name</i> —Name of the version 9 template.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates</a> ” on page 1156.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## template-id

---

<b>Syntax</b>	template-id <i>id</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring version9 template</a> <i>template-name</i> ] [edit <a href="#">services flow-monitoringversion-ipfix template</a> <i>template-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 14.1.
<b>Description</b>	Define a template ID to be used for flow aggregation of version 9 and IPFIX flows. If you do not configure values for the template ID and options template ID, default values are assumed for these IDs, which are different for the various address families. If you configure the same template ID or options template ID value for different address families, such a setting is not processed properly and might cause unexpected behavior. For example, if you configure the same template ID value for both IPv4 and IPv6, the collector validates the export data based on the template ID value that it last receives. In this case, if IPv6 is configured after IPv4, the value is effective for IPv6 and the default value is used for IPv4.
<b>Options</b>	<i>id</i> —Specify a unique identifier for the template to be used for version 9 or IPFIX flows. <b>Range:</b> 1024 through 65535
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows on page 1172</a></li><li>• <a href="#">Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 1167</a></li></ul>

## template-refresh-rate

<b>Syntax</b>	template-refresh-rate packets <i>packets</i> seconds <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring version9 template <i>template-name</i></a> ] [edit <a href="#">services flow-monitoring version-ipfix template <i>template-name</i></a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. Support at the [edit <a href="#">services flow-monitoring version-ipfix template <i>template-name</i></a> ] hierarchy level added in Junos OS Release 10.2.
<b>Description</b>	Specify the refresh rate, in either packets or seconds.
<b>Options</b>	<i>packets</i> —Refresh rate, in number of packets. <b>Range:</b> 1 through 480,000 <b>Default:</b> 4800  <i>seconds</i> —Refresh rate, in number of seconds. <b>Range:</b> 10 through 600 <b>Default:</b> 600
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156</a></li> </ul>

## traceoptions (Forwarding Options)

<b>Syntax</b>	traceoptions { no-remote-trace; file <i>filename</i> <files <i>number</i> > <size <i>bytes</i> > <match <i>expression</i> > <world-readable   no-world-readable>; }
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options port-mirroring</a> ], [edit <a href="#">forwarding-options sampling</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure traffic sampling tracing operations.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Tracing Traffic Sampling Operations on page 1140</a></li> </ul>

## unit

---

**Syntax**    `unit logical-unit-number {  
              family inet {  
                  address address {  
                    destination destination-address;  
                  }  
                  filter {  
                    group filter-group-number;  
                    input filter-name;  
                    output filter-name;  
                  }  
                  sampling direction;  
              }  
          }`

**Hierarchy Level**    [edit [interfaces](#) *interface-name*]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

**Options**    *logical-unit-number*—Number of the logical unit.

**Range:** 0 through 16,384

The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Network Interfaces Library for Routing Devices* for other statements that do not affect services interfaces.
- *Junos OS Network Interfaces Library for Routing Devices*

## version

---

<b>Syntax</b>	<code>version <i>format</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options accounting</a> <i>name</i> <a href="#">output flow-server</a> <i>hostname</i> ], [edit <a href="#">forwarding-options sampling instance</a> <i>instance-name</i> <a href="#">family</a> (inet   inet6   mpls) <a href="#">output flow-server</a> <i>hostname</i> ], [edit <a href="#">forwarding-options sampling family</a> (inet   inet6   mpls) <a href="#">output flow-server</a> <i>hostname</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the version format of the aggregated flows exported to a cflowd server.
<b>Options</b>	<i>format</i> —Format of the flows. <b>Values:</b> 5 or 8 <b>Default:</b> 5
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">export-format on page 1227</a></li><li>• <a href="#">Enabling Flow Aggregation on page 1151</a></li></ul>

## version9

---

See the following sections:

- [version9 \(Forwarding Options\) on page 1290](#)
- [version9 \(Services\) on page 1291](#)

### version9 (Forwarding Options)

<b>Syntax</b>	<pre>version9 {     <a href="#">template</a> <i>template-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options sampling instance</a> <i>instance-name</i> <a href="#">family</a> (inet   inet6   mpls) <a href="#">output flow-server</a> <i>hostname</i> ], [edit <a href="#">forwarding-options sampling family</a> (inet   inet6   mpls) <a href="#">output flow-server</a> <i>hostname</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	Specify flow monitoring version 9 properties to apply to output sampling records. The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates on page 1156</a></li></ul>

**version9 (Services)**

**Syntax**

```

version9 {
  template template-name {
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    ipv4-template;
    ipv6-template;
    mpls-template {
      label-position [ positions ];
    }
    mpls-ipv4-template {
      label-position [ positions ];
    }
    peer-as-billing-template;
    option-refresh-rate packets packets seconds seconds;
    template-refresh-rate packets packets seconds seconds;
  }
}

```

**Hierarchy Level** [edit [services flow-monitoring](#)]

**Release Information** Statement introduced in Junos OS Release 8.3.

**Description** Specify flow aggregation version 9 template properties. The remaining statements are explained separately.

**Usage Guidelines** See “[Configuring Flow Aggregation to Use Version 9 Flow Templates](#)” on page 1156.

**Required Privilege Level** interface—To view this statement in the configuration.  
 interface-control—To add this statement to the configuration.

## version-ipfix

---

See the following sections:

- [version-ipfix \(Forwarding Options\) on page 1292](#)
- [version-ipfix \(Services\) on page 1293](#)

### version-ipfix (Forwarding Options)

<b>Syntax</b>	<code>version-ipfix {     template <i>template-name</i>; }</code>
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options sampling</a> instance <i>instance-name</i> family inet <a href="#">output</a> flow-server <i>address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the output format to support inline flow monitoring.
<b>Options</b>	<i>template-name</i> —Currently <b>ipv4</b> is the only output template format supported.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">export-format on page 1227</a></li><li>• <a href="#">Configuring Inline Sampling on page 1176</a></li></ul>

## version-ipfix (Services)

<b>Syntax</b>	<pre> version-ipfix {   template <i>template-name</i> {     flow-active-timeout <i>seconds</i>;     flow-inactive-timeout <i>seconds</i>;     ipv4-template;     ipv6-template;     option-refresh-rate <i>packets packets seconds seconds</i>;     template-refresh-rate <i>packets packets seconds seconds</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services flow-monitoring</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2. Statement introduced in Junos OS Release 12.R3 for EX Series switches.
<b>Description</b>	Specify the output template properties to support inline flow monitoring. The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Inline Sampling</a> ” on page 1176.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## world-readable

<b>Syntax</b>	(world-readable   no-world-readable);
<b>Hierarchy Level</b>	[edit <a href="#">forwarding-options port-mirroring traceoptions file</a> ], [edit <a href="#">forwarding-options sampling family</a> (inet   inet6   impls) <a href="#">output file</a> ], [edit <a href="#">forwarding-options sampling traceoptionsfile</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Enable unrestricted file access.
<b>Options</b>	<b>no-world-readable</b> —Restrict file access to owner. This is the default.  <b>world-readable</b> —Enable unrestricted file access. <b>Default:</b> no-world-readable
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Port Mirroring on page 1186</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> </ul>



# Flow Collection Configuration Guidelines

You can process and export multiple cflowd records with a flow collector interface. You create a flow collector interface on a Monitoring Services II or Multiservices 400 PIC. The flow collector interface combines multiple cflowd records into a compressed ASCII data file and exports the file to an FTP server. To convert a services PIC into a flow collector interface, include the **flow-collector** statement at the **[edit chassis fpc fpc-slot pic pic-slot monitoring-services application]** hierarchy level.

You can use the services PIC for either flow collection or monitoring, but not for both types of service simultaneously. When converting the PIC between service types, you must configure the **flow-collector** statement, take the PIC offline, and then bring the PIC back online. Restarting the router does not enable the new service type.

A flow collector interface, designated by the **cp-fpc/pic/port** interface name, requires three logical interfaces for correct operation. Units 0 and 1 are used to send the compressed ASCII data files to an FTP server, while Unit 2 is used to receive cflowd records from a monitoring services interface.



**NOTE:** Unlike conventional interfaces, the **address** statement at the **[edit interfaces cp-fpc/pic/port unit unit-number family inet]** hierarchy level corresponds to the IP address of the Routing Engine. Likewise, the **destination** statement at the **[edit interfaces cp-fpc/pic/port unit unit-number family inet address ip-address]** hierarchy level corresponds to the IP address of the flow collector interface. As a result, you must configure the **destination** statement for Unit 0 and 1 with *local* addresses that can reach the FTP server. Similarly, configure the **destination** statement for Unit 2 with a *local* IP address so it can reach the monitoring services interface that sends cflowd records.

To activate flow collector services after the services PIC is converted into a flow collector, include the **flow-collector** statement at the **[edit services]** hierarchy level. After you activate the flow collector, you need to configure the following components:

- Destination of the FTP server
- File specifications
- Input interface-to-flow collector interface mappings
- Transfer log settings

To configure flow collection, include the **flow-collector** statement at the **[edit services]** hierarchy level:

```
flow-collector {
  analyzer-address address;
  analyzer-id name;
  destinations {
    ftp:url {
      password "password";
    }
    file-specification {
      variant variant-number {
        data-format format;
        name-format format;
        transfer {
          record-level number;
          timeout seconds;
        }
      }
    }
  }
  interface-map {
    collector interface-name;
    file-specification variant-number;
    interface-name {
      collector interface-name;
      file-specification variant-number;
    }
  }
  retry number;
  retry-delay seconds;
  transfer-log-archive {
    archive-sites {
      ftp:url {
        password "password";
        username username;
      }
    }
    filename-prefix prefix;
    maximum-age minutes;
  }
}
```

This chapter contains the following sections:

- [Configuring Flow Collection on page 1297](#)
- [Sending cflowd Records to Flow Collector Interfaces on page 1300](#)
- [Configuring Flow Collection Mode and Interfaces on Services PICs on page 1300](#)
- [Example: Configuring Flow Collection on page 1301](#)

## Configuring Flow Collection

This section describes the following tasks for configuring flow collection:

- [Configuring Destination FTP Servers for Flow Records on page 1297](#)
- [Configuring a Packet Analyzer on page 1297](#)
- [Configuring File Formats on page 1298](#)
- [Configuring Interface Mappings on page 1298](#)
- [Configuring Transfer Logs on page 1299](#)
- [Configuring Retry Attempts on page 1299](#)

### Configuring Destination FTP Servers for Flow Records

Flow collection destinations are where the compressed ASCII data files are sent after the cflowd records are collected and processed. To specify the destination FTP server, include the **destinations** statement at the **[edit services flow-collector]** hierarchy level. You can specify up to two FTP server destinations and include the password for each configured server. If two FTP servers are configured, the first server in the configuration is the primary server and the second is a backup server.

To configure a destination for flow collection files, include the **destinations** statement at the **[edit services flow-collector]** hierarchy level:

```
[edit services flow-collector]
destinations {
  ftp:url {
    password "password";
  }
}
```

To specify the destination FTP server, include the **ftp:url** statement. The value **url** is the FTP server address for the primary flow collection destination and can include macros.

When you include macros in the **ftp:url** statement, a directory can be created only for a single level. For example, the path **ftp://10.2.2.2/%m/%Y** expands to **ftp://10.2.2.2/01/2005**, and the software attempts to create the directory **01/2005** on the destination FTP server. If the **01/** directory already exists on the destination FTP server, the software creates the **/2005/ directory** one level down. If the **01/** directory does not exist on the destination FTP server, the software cannot create the **/2005/ directory**, and the FTP server destination will fail. For more information about macros, see [ftp](#).

To specify the FTP server password, include the **password "password"** statement. The password must be enclosed in quotation marks. You can specify up to two destination FTP servers. The first destination specified is considered the primary destination.

### Configuring a Packet Analyzer

You can specify values for the IP address and identifier of a packet analyzer to which the flow collector interface sends traffic for analysis. The values you specify here override any default values configured elsewhere.

To configure an IP address and identifier for the packet analyzer, include the **analyzer-address** and **analyzer-id** statements at the **[edit services flow-collector]** hierarchy level:

```
[edit services flow-collector]
analyzer-address address;
analyzer-id name;
```

## Configuring File Formats

You configure data file formats, name formats, and transfer characteristics for the flow collection files. File records are sent to the destination FTP server when the timer expires or when a preset number of records are received, whichever comes first.

To configure the flow collection file format, include the **file-specification** statement at the **[edit services flow-collector]** hierarchy level:

```
[edit services flow-collector]
file-specification {
  variant variant-number {
    data-format format;
    name-format format;
    transfer {
      record-level number;
      timeout seconds;
    }
  }
}
```

To set the data file format, include the **data-format** statement. To set the file name format, include the **name-format** statement. To set the export timer and file size thresholds, include the **transfer** statement and specify values for the **timeout** and **record-level** options.

For example, you can specify the name format as follows:

```
[edit services flow-collector file-specification variant variant-number]
name-format "cFlowd-py69Ni69-0-%D_%T-%I_%N.bcp.bi.gz";
```

In this example, **cFlowd-py69Ni69-0** is the static portion used verbatim, **%D** is the date in YYYYMMDD format, **%T** is the time in HHMMSS format, **%I** is the value of **ifAlias**, **%N** is the generation number, and **bcp.bi.gz** is a user-configured string. A number of macros are supported for expressing the date and time information in different ways; for a complete list, see the summary section for **name-format**.

## Configuring Interface Mappings

You can match an input interface with a flow collector interface and apply the preset file specifications to the input interface.

To configure an interface mapping, include the **interface-map** statement at the **[edit services flow-collector]** hierarchy level:

```
[edit services flow-collector]
interface-map {
```

```

collector interface-name;
file-specification variant-number;
interface-name {
    collector interface-name;
    file-specification variant-number;
}
}

```

To configure the default flow collector and file specifications for all input interfaces, include the **file-specification** and **collector** statements at the **[edit services flow-collector interface-map]** hierarchy level. To override the default settings and apply flow collector and file specifications to a specific input interface, include the **file-specification** and **collector** statements at the **[edit services flow-collector interface-map interface-name]** hierarchy level.

## Configuring Transfer Logs

You can configure the filename, export interval, maximum size, and destination FTP server for log files containing the transfer activity history for a flow collector interface.

To configure a transfer log, include the **transfer-log-archive** statement at the **[edit services flow-collector]** hierarchy level:

```

[edit services flow-collector]
transfer-log-archive {
    archive-sites {
        ftp:url {
            password "password";
            username username;
        }
    }
    filename-prefix prefix;
    maximum-age minutes;
}

```

To configure the destination for archiving files, include the **archive-sites** statement. Specify the filename as follows:

```

[edit services flow-collector transfer-log]
filename "cFlowd-py69Ni69-0-%D_%T";

```

where **cFlowd-py69Ni69-0** is the static portion used verbatim, **%D** is the date in YYYYMMDD format, and **%T** is the time in HHMMSS format.

You can optionally include the following statements:

- **filename-prefix**—Sets a standard prefix for all the logged files.
- **maximum-age**—Specifies the duration a file remains on the server. The range is 1 through 360 minutes.

## Configuring Retry Attempts

You can specify values for situations in which the flow collector interface needs more than one attempt to transfer log files to the FTP server:

- Maximum number of retry attempts
- Amount of time the flow collector interface waits between successive retries

To configure retry settings, include the **retry** and **retry-delay** statements at the **[edit services flow-collector]** hierarchy level:

```
retry number;  
retry-delay seconds;
```

The **retry** value can be from 0 through 10. The **retry-delay** value can be from 0 through 60 seconds.

**Related  
Documentation**

- [Flow Collection Overview](#)
- [Sending cflowd Records to Flow Collector Interfaces on page 1300](#)
- [Configuring Flow Collection Mode and Interfaces on Services PICs on page 1300](#)
- [Example: Configuring Flow Collection on page 1301](#)

---

## Sending cflowd Records to Flow Collector Interfaces

To specify a flow collector interface as the destination for cflowd records coming from a services PIC, include the **collector-pic** statement at the **[edit forwarding-options monitoring group-name family inet output flow-export-destination]** hierarchy level:

```
[edit forwarding-options monitoring group-name family inet output flow-export-destination]  
collector-pic;
```

You can select either the flow collector interface or a cflowd server as the destination for cflowd records, but not both at the same time.

**Related  
Documentation**

- [Flow Collection Overview](#)
- [Configuring Flow Collection on page 1297](#)
- [Configuring Flow Collection Mode and Interfaces on Services PICs on page 1300](#)
- [Example: Configuring Flow Collection on page 1301](#)

---

## Configuring Flow Collection Mode and Interfaces on Services PICs

You can select the services PIC to run in either flow collection mode or monitoring mode, but not both.

To set the services PIC to run in flow collection mode, include the **flow-collector** statement at the **[edit chassis fpc slot-number pic pic-number monitoring-services application]** hierarchy level:

```
[edit chassis fpc slot-number pic pic-number monitoring-services application]  
flow-collector;
```

For further information on configuring chassis properties, see the *Junos OS Administration Library for Routing Devices*.

To specify flow collection interfaces, you configure the **cp** interface at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
cp-fpc/pic/port {
  ...
}
```

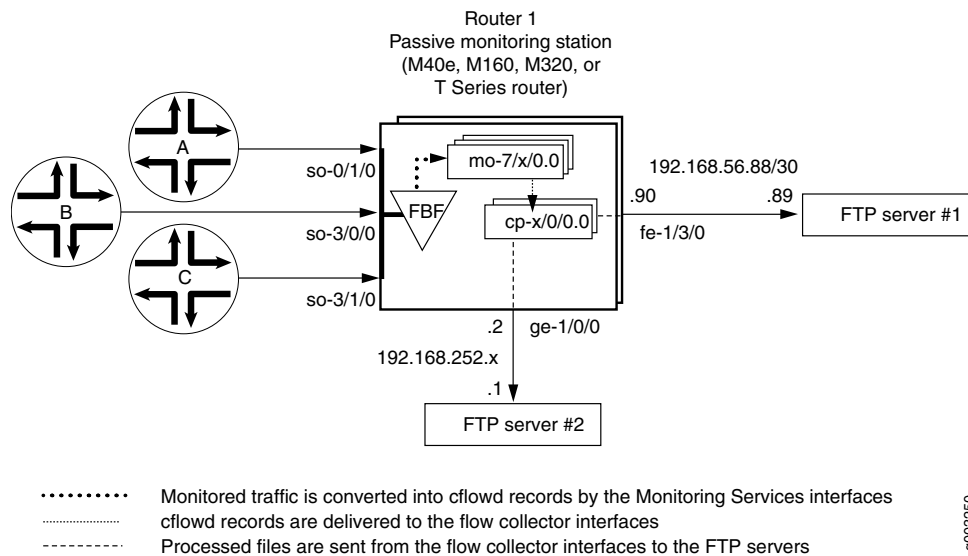
#### Related Documentation

- [Flow Collection Overview](#)
- [Configuring Flow Collection on page 1297](#)
- [Sending cflowd Records to Flow Collector Interfaces on page 1300](#)
- [Example: Configuring Flow Collection on page 1301](#)

## Example: Configuring Flow Collection

Figure 23 on page 1301 shows the path traveled by monitored traffic as it passes through the router. Packets arrive at input interfaces **so-0/1/0**, **so-3/0/0**, and **so-3/1/0**. The raw packets are directed into a filter-based forwarding routing instance and processed into cflowd records by the monitoring services interfaces **mo-7/1/0**, **mo-7/2/0**, and **mo-7/3/0**. The cflowd records are compressed into files at the flow collector interfaces **cp-6/0/0** and **cp-7/0/0** and sent to the FTP server for analysis. Finally, a mandatory class-of-service (CoS) configuration is applied to export channels 0 and 1 on the flow collector interfaces to manage the outgoing processed files.

Figure 23: Flow Collector Interface Topology Diagram



```
[edit]
chassis {
  fpc 6 {
    pic 0 {
      monitoring-services {
        application flow-collector; # This converts a Monitoring Services II or
```

```

        # Multiservices 400 PIC into a flow collector interface.
    }
}
}
fpc 7 {
    pic 0 {
        monitoring-services {
            application flow-collector; # This converts a Monitoring Services II or
            # Multiservices 400 PIC into a flow collector interface.
        }
    }
}
}
}
interfaces {
    cp-6/0/0 {
        unit 0 { # Logical interface .0 on a flow collector interface is export
            family inet { # channel 0 and sends records to the FTP server.
                filter {
                    output cp-ftp; # Apply the CoS filter here.
                }
                address 10.0.0.1/32 {
                    destination 10.0.0.2;
                }
            }
        }
        unit 1 { # Logical interface .1 on a flow collector interface is export
            family inet { # channel 1 and sends records to the FTP server.
                filter {
                    output cp-ftp; # Apply the CoS filter here.
                }
                address 10.1.1.1/32 {
                    destination 10.1.1.2;
                }
            }
        }
        unit 2 { # Logical interface .2 on a flow collector interface is the flow
            family inet { # receive channel that communicates with the Routing Engine.
                address 10.2.2.1/32 { # Do not apply a CoS filter on logical interface .2.
                    destination 10.2.2.2;
                }
            }
        }
    }
}
cp-7/0/0 {
    unit 0 { # Logical interface .0 on a flow collector interface is export
        family inet { # channel 0 and sends records to the FTP server.
            filter {
                output cp-ftp; # Apply the CoS filter here.
            }
            address 10.3.3.1/32 {
                destination 10.3.3.2;
            }
        }
    }
    unit 1 { # Logical interface .1 on a flow collector interface is export
        family inet { # channel 1 and sends records to the FTP server.

```

```

        filter {
            output cp-ftp;# Apply the CoS filter here.
        }
        address 10.4.4.1/32 {
            destination 10.4.4.2;
        }
    }
}
unit 2 {# Logical interface .2 on a flow collector interface is the flow
    family inet {# receive channel that communicates with the Routing Engine.
        address 10.5.5.1/32 {# Do not apply a CoS filter on logical interface .2.
            destination 10.5.5.2;
        }
    }
}
}
fe-1/3/0 { # This is the exit interface leading to the first FTP server.
    unit 0 {
        family inet {
            address 192.168.56.90/30;
        }
    }
}
ge-1/0/0 { # This is the exit interface leading to the second FTP server.
    unit 0 {
        family inet {
            address 192.168.252.2/24;
        }
    }
}
mo-7/1/0 { # This is the first interface that creates cflowd records.
    unit 0 {
        family inet;
    }
}
mo-7/2/0 { # This is the second interface that creates cflowd records.
    unit 0 {
        family inet;
    }
}
mo-7/3/0 { # This is the third interface that creates cflowd records.
    unit 0 {
        family inet;
    }
}
so-0/1/0 { # This is the first input interface that receives traffic to be monitored.
    encapsulation ppp;
    unit 0 {
        passive-monitor-mode; # This allows the interface to be passively monitored.
        family inet {
            filter {
                input catch; # The filter-based forwarding filter is applied here.
            }
        }
    }
}
}

```

```

so-3/0/0 { # This is the second interface that receives traffic to be monitored.
  encapsulation ppp;
  unit 0 {
    passive-monitor-mode; # This allows the interface to be passively monitored.
    family inet {
      filter {
        input catch; # The filter-based forwarding filter is applied here.
      }
    }
  }
}
so-3/1/0 { # This is the third interface that receives traffic to be monitored.
  encapsulation ppp;
  unit 0 {
    passive-monitor-mode; # This allows the interface to be passively monitored.
    family inet {
      filter {
        input catch; # The filter-based forwarding filter is applied here.
      }
    }
  }
}
forwarding-options {
  monitoring group1 { # Always define your monitoring group here.
    family inet {
      output {
        export-format cflowd-version-5;
        flow-active-timeout 60;
        flow-inactive-timeout 15;
        flow-export-destination collector-pic; # Sends records to the flow collector.
        interface mo-7/1/0.0 {
          source-address 192.168.252.2;
        }
        interface mo-7/2/0.0 {
          source-address 192.168.252.2;
        }
        interface mo-7/3/0.0 {
          source-address 192.168.252.2;
        }
      }
    }
  }
}
firewall {
  family inet {
    filter cp-ftp { # This filter provides CoS for flow collector interface traffic.
      term t1 {
        then forwarding-class expedited-forwarding;
      }
    }
  }
}
filter catch { # This firewall filter sends incoming traffic into the
  interface-specific; # filter-based forwarding routing instance.
  term def {
    then {
      count counter;
      routing-instance fbf_instance;
    }
  }
}

```

```

    }
  }
}
routing-options {
  interface-routes {
    rib-group inet common;
  }
  rib-groups {
    common {
      import-rib [inet.0 fbf_instance.inet.0];
    }
  }
  forwarding-table {
    export pplb;
  }
}
policy-options {
  policy-statement pplb {
    then {
      load-balance per-packet;
    }
  }
}
routing-instances {
  fbf_instance { # This instance sends traffic to the monitoring services interface.
    instance-type forwarding;
    routing-options {
      static {
        route 0.0.0.0/0 next-hop mo-7/1/0.0;
      }
    }
  }
}
class-of-service { # A class-of-service configuration for the flow collector interface
  interfaces { # is required for flow collector services.
    cp-6/0/0 {
      scheduler-map cp-map;
    }
    cp-7/0/0 {
      scheduler-map cp-map;
    }
  }
}
scheduler-maps {
  cp-map {
    forwarding-class best-effort scheduler Q0;
    forwarding-class expedited-forwarding scheduler Q1;
    forwarding-class network-control scheduler Q3;
  }
}
schedulers {
  Q0 {
    transmit-rate remainder;
    buffer-size percent 90;
  }
}

```

```

Q1 {
    transmit-rate percent 5;
    buffer-size percent 5;
    priority strict-high;
}
Q3 {
    transmit-rate percent 5;
    buffer-size percent 5;
}
}
services {
    flow-collector { # Define properties for flow collector interfaces here.
        analyzer-address 10.10.10.1; # This is the IP address of the analyzer.
        analyzer-id server1; # This helps to identify the analyzer.
        retry 3; # Maximum number of attempts by the PIC to send a file transfer log.
        retry-delay 30; # The time interval between attempts to send a file transfer log.
        destinations { # This defines the FTP servers that receive flow collector output.
            "ftp://user@192.168.56.89//tmp/collect1/" { # The primary FTP server.
                password "$9$IJK8xN-w2oZdbZDHmF30O1"; # SECRET-DATA
            }
            "ftp://user@192.168.252.1//tmp/collect2/" { # The secondary FTP server.
                password "$9$elbvL7-dsgaGVwGjkP3nOBI"; # SECRET-DATA
            }
        }
    }
    file-specification { # Define sets of flow collector characteristics here.
        def-spec {
            name-format "default-allInt-0-%D_%T-%l_%N.bcp.bi.gz";
            data-format flow-compressed; # The default compressed output format.
        } # When no overrides are specified, a collector uses default transfer values.
        f1 {
            name-format "cFlowd-py69Ni69-0-%D_%T-%l_%N.bcp.bi.gz";
            data-format flow-compressed; # The default compressed output format.
            transfer timeout 1800 record-level 1000000; # Here are configured values.
        }
    }
    interface-map { # Allows you to map interfaces to flow collector interfaces.
        file-specification def-spec; # Flows generated for default traffic are sent to the
        collector cp-7/0/0; # default flow collector interface "cp-7/0/0".
        so-0/1/0.0 { # Flows generated for the so-0/1/0 interface are sent
            collector cp-6/0/0; # to cp-6/0/0, and the file-specification used is
        } # "default."
        so-3/0/0.0 { # Flows generated for the so-3/0/0 interface are sent
            file-specification f1; # to cp-6/0/0, and the file-specification used is "f1."
            collector cp-6/0/0;
        }
        so-3/1/0.0; # Because no settings are defined, flows generated for this
    } # interface use interface cp-7/0/0 and the default file specification.
    transfer-log-archive { # Sends flow collector interface log files to an FTP server.
        filename-prefix so_3_0_0_log;
        maximum-age 15;
        archive-sites {
            "ftp://user@192.168.56.89//tmp/transfers/" {
                password "$9$IFaEyevMXNVsWLsgaU.m6/C";
            }
        }
    }
}
]

```

```
}  
}
```

**Related  
Documentation**

- *Flow Collection Overview*
- [Configuring Flow Collection on page 1297](#)
- [Sending cflowd Records to Flow Collector Interfaces on page 1300](#)
- [Configuring Flow Collection Mode and Interfaces on Services PICs on page 1300](#)



## CHAPTER 53

# Summary of Flow Collection Configuration Statements

The following sections explain each of the flow collection configuration statements. The statements are organized alphabetically.

### analyzer-address

---

<b>Syntax</b>	<code>analyzer-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit services flow-collector]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure an IP address for the packet analyzer that overrides the default value.
<b>Options</b>	<i>address</i> —IP address for packet analyzer.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Packet Analyzer on page 1297</a></li></ul>

## analyzer-id

---

<b>Syntax</b>	<code>analyzer-id <i>name</i>;</code>
<b>Hierarchy Level</b>	[edit services flow-collector]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure an identifier for the packet analyzer that overrides the default value.
<b>Options</b>	<i>name</i> —Identifier for packet analyzer.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a Packet Analyzer on page 1297</a></li></ul>

## archive-sites

---

<b>Syntax</b>	<pre>archive-sites {   ftp:url {     password "<i>password</i>";     username <i>username</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit services flow-collector <a href="#">transfer-log-archive</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the destination for transfer logs.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Transfer Logs on page 1299</a></li></ul>

## collector

---

<b>Syntax</b>	<code>collector <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit services flow-collector interface-map]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the default flow collector interface for interface mapping.
<b>Options</b>	<i>interface-name</i> —Default flow collector interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Interface Mappings on page 1298</a></li></ul>

## data-format

---

<b>Syntax</b>	<code>data-format <i>format</i>;</code>
<b>Hierarchy Level</b>	[edit services flow-collector file-specification variant <i>variant-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the data format for a specific file format variant.
<b>Options</b>	<i>format</i> —Data format. Specify <b>flow-compressed</b> as the data format.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring File Formats on page 1298</a></li></ul>

## destinations

---

<b>Syntax</b>	<pre>destinations {   ftp:url {     password "password";   } }</pre>
<b>Hierarchy Level</b>	[edit services flow-collector]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the primary and secondary destination FTP servers.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Destination FTP Servers for Flow Records on page 1297</a></li></ul>

## filename-prefix

---

<b>Syntax</b>	<pre>filename-prefix <i>prefix</i>;</pre>
<b>Hierarchy Level</b>	[edit services flow-collector transfer-log-archive]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the filename prefix for log files.
<b>Options</b>	<i>prefix</i> —Filename identifier.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Transfer Logs on page 1299</a></li></ul>

## file-specification

See the following sections:

- [file-specification \(File Format\) on page 1313](#)
- [file-specification \(Interface Mapping\) on page 1313](#)

### file-specification (File Format)

<b>Syntax</b>	<pre>file-specification {     variant <i>variant-number</i> {         data-format <i>format</i>;         name-format <i>format</i>;         transfer {             record-level <i>number</i>;             timeout <i>seconds</i>;         }     } }</pre>
<b>Hierarchy Level</b>	[edit services flow-collector]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the file format for the flow collection files.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring File Formats on page 1298</a></li> </ul>

### file-specification (Interface Mapping)

<b>Syntax</b>	<pre>file-specification {     variant <i>variant-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit services flow-collector interface-map]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the default file specification for interface mapping.
<b>Options</b>	<i>variant-number</i> —Default file format variant.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## flow-collector

```

Syntax  flow-collector {
        analyzer-address address;
        analyzer-id name;
        destinations {
            ftp:url {
                password "password";
            }
        }
        file-specification {
            variant variant-number {
                data-format format;
                name-format format;
                transfer {
                    record-level number;
                    timeout seconds;
                }
            }
        }
        interface-map {
            collector interface-name;
            file-specification variant-number;
            interface-name {
                collector interface-name;
                file-specification variant-number;
            }
        }
        retry number;
        retry-delay seconds;
        transfer-log-archive {
            archive-sites {
                ftp:url {
                    password "password";
                    username username;
                }
            }
            filename-prefix prefix;
            maximum-age minutes;
        }
    }

```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the flow collection.

**Options** The statements are explained separately.

**Required Privilege** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.

**Related Documentation** • *Flow Collection*

## ftp

---

See the following sections:

- [ftp \(Flow Collector Files\)](#) on page 1317
- [ftp \(Transfer Log Files\)](#) on page 1318

## ftp (Flow Collector Files)

<b>Syntax</b>	<code>ftp:url;</code>
<b>Hierarchy Level</b>	[edit services flow-collector destination]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the primary and secondary destination FTP server addresses.
<b>Options</b>	<p><b>url</b>—FTP server address. The URL can include the following macros, typed in braces:</p> <ul style="list-style-type: none"> <li>• <b>{%D}</b>—Date</li> <li>• <b>{%T}</b>—Time when the file is created</li> <li>• <b>{%I}</b>—Description string for the logical interface configured using the collector <i>interface-name</i> statement at the [edit services flow-collector interface-map] hierarchy</li> <li>• <b>{%N}</b>—Unique, sequential number for each new file created</li> <li>• <b>{am_pm}</b>—AM or PM</li> <li>• <b>{date}</b>—Current date using the {year} {month} {day} macros</li> <li>• <b>{day}</b>—From 01 through 31</li> <li>• <b>{day_abbrev}</b>—Sun through Sat</li> <li>• <b>{day_full}</b>—Sunday through Saturday</li> <li>• <b>{generation number}</b>—Unique, sequential number for each new file created</li> <li>• <b>{hour_12}</b>—From 01 through 12</li> <li>• <b>{hour_24}</b>—From 00 through 23</li> <li>• <b>{ifalias}</b>—Description string for the logical interface configured using the collector statement at the [edit services flow-collector interface-map] hierarchy</li> <li>• <b>{minute}</b>—From 00 through 59</li> <li>• <b>{month}</b>—From 01 through 12</li> <li>• <b>{month_abbrev}</b>—Jan through Dec</li> <li>• <b>{month_full}</b>—January through December</li> <li>• <b>{num_zone}</b>—From -2359 to +2359; this macro is not supported</li> <li>• <b>{second}</b>—From 00 through 60</li> <li>• <b>{time}</b>—Time the file is created, using the {hour_24} {minute} {second} macros</li> <li>• <b>{time_zone}</b>—Time zone code name of the locale; for example, <b>gmt</b> (this macro is not supported).</li> <li>• <b>{year}</b>—In the format YYYY; for example, 1970</li> <li>• <b>{year_abbrev}</b>—From 00 through 99</li> </ul>

**Required Privilege** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Destination FTP Servers for Flow Records on page 1297](#)

## ftp (Transfer Log Files)

**Syntax** `ftp:url;`

**Hierarchy Level** [edit services flow-collector [transfer-log-archive archive-sites](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Specify the primary and secondary destination FTP server addresses.

**Options** `url`—FTP server address.

**Required Privilege** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Transfer Logs on page 1299](#)

---

## interface-map

**Syntax**

```
interface-map {
  collector interface-name;
  file-specification variant-number;
  interface-name {
    collector interface-name;
    file-specification variant-number;
  }
}
```

**Hierarchy Level** [edit services flow-collector]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Match an input interface with a flow collector interface and apply the preset file specifications to the input interface.

**Options** The statements are explained separately.

**Required Privilege** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Interface Mappings on page 1298](#)

## maximum-age

---

<b>Syntax</b>	maximum-age <i>minutes</i> ;
<b>Hierarchy Level</b>	[edit services flow-collector <a href="#">transfer-log-archive</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Maximum age of transfer log file.
<b>Options</b>	<b>maximum-age <i>minutes</i></b> —Transfer log file age. <b>Range:</b> 1 through 360
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Transfer Logs on page 1299</a></li></ul>

## name-format

---

<b>Syntax</b>	<code>name-format "format";</code>
<b>Hierarchy Level</b>	[edit services flow-collector file-specification variant <i>variant-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the name format for a specific file format. The files may include supported macros. Use macros to organize files on the external machine to which they are exported from the collector PIC.
<b>Options</b>	<p><i>format</i>—Specify the filename format, within quotation marks. The name format can include the following macros, typed in braces:</p> <ul style="list-style-type: none"><li>• <code>{%D}</code>—Date</li><li>• <code>{%T}</code>—Time when the file is created</li><li>• <code>{%I}</code>—Description string for the logical interface configured using the <b>collector</b> statement at the [edit services flow-collector interface-map] hierarchy level</li><li>• <code>{%N}</code>—Unique, sequential number for each new file created</li><li>• <code>{am_pm}</code>—AM or PM</li><li>• <code>{date}</code>—Current date using the <code>{year}</code> <code>{month}</code> <code>{day}</code> macros</li><li>• <code>{day}</code>—From 01 through 31</li><li>• <code>{day_abbrev}</code>—Sun through Sat</li><li>• <code>{day_full}</code>—Sunday through Saturday</li><li>• <code>{generation number}</code>—Unique, sequential number for each new file created</li><li>• <code>{hour_12}</code>—From 01 through 12</li><li>• <code>{hour_24}</code>—From 00 through 23</li><li>• <code>{ifalias}</code>—Description string for the logical interface configured using the <b>collector</b> statement at the [edit services flow-collector interface-map] hierarchy level</li><li>• <code>{minute}</code>—From 00 through 59</li><li>• <code>{month}</code>—From 01 through 12</li><li>• <code>{month_abbrev}</code>—Jan through Dec</li><li>• <code>{month_full}</code>—January through December</li><li>• <code>{num_zone}</code>—From -2359 through +2359; this macro is not supported</li><li>• <code>{second}</code>—From 00 through 60</li><li>• <code>{time}</code>—Time the file is created, using the <code>{hour_24}</code> <code>{minute}</code> <code>{second}</code> macros</li><li>• <code>{time_zone}</code>—Time zone code name of the locale; for example, <code>gmt</code> (this macro is not supported).</li></ul>

- **{year}**—In the format YYYY; for example, 1970
- **{year\_abbrev}**—From 00 through 99

<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring File Formats on page 1298</a></li></ul>
------------------------------	---

## password

---

See the following sections:

- [password \(Flow Collector File Servers\) on page 1322](#)
- [password \(Transfer Log File Servers\) on page 1322](#)

### password (Flow Collector File Servers)

<b>Syntax</b>	<code>password "password";</code>
<b>Hierarchy Level</b>	[edit services flow-collector destination ftp:url]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the primary and secondary destination FTP server password.
<b>Options</b>	<i>password</i> —FTP server password.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Destination FTP Servers for Flow Records on page 1297</a></li></ul>

### password (Transfer Log File Servers)

<b>Syntax</b>	<code>password "password";</code>
<b>Hierarchy Level</b>	[edit services flow-collector transfer-log-archive archive-sites]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the primary and secondary destination FTP server password.
<b>Options</b>	<i>password</i> —FTP server password.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Transfer Logs on page 1299</a></li></ul>

## retry (Services Flow Collector)

---

<b>Syntax</b>	<code>retry number;</code>
<b>Hierarchy Level</b>	[edit services flow-collector]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the maximum number of attempts the flow collector interface will make to transfer log files to the FTP server.
<b>Options</b>	<i>number</i> —Maximum number of transfer retry attempts. <b>Range:</b> 0 through 10
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Retry Attempts on page 1299</a></li></ul>

## retry-delay

---

<b>Syntax</b>	<code>retry-delay seconds;</code>
<b>Hierarchy Level</b>	[edit services flow-collector]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the amount of time the flow collector interface waits between retry attempts.
<b>Options</b>	<i>seconds</i> —Amount of time between transfer retry attempts. <b>Range:</b> 0 through 60
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Retry Attempts on page 1299</a></li></ul>

## transfer

---

<b>Syntax</b>	<pre>transfer {     record-level <i>number</i>;     timeout <i>seconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit services flow-collector file-specification variant <i>variant-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify when to send the flow collection file. The file is sent when either of the two conditions is met.
<b>Options</b>	<p><b>record-level <i>number</i></b>—Number of flow collection files collected.</p> <p><b>timeout <i>seconds</i></b>—Timeout duration.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring File Formats on page 1298</a></li></ul>

## transfer-log-archive

---

<b>Syntax</b>	<pre>transfer-log-archive {     archive-sites {         ftp:url {             password "<i>password</i>";             username <i>username</i>;         }     }     filename-prefix <i>prefix</i>;     maximum-age <i>minutes</i>; }</pre>
<b>Hierarchy Level</b>	[edit services flow-collector]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the filename prefix, maximum age, and destination FTP server for log files containing the transfer activity history for a flow collector interface.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Transfer Logs on page 1299</a></li></ul>

## username (Services)

---

<b>Syntax</b>	<code>username <i>user-name</i>;</code>
<b>Hierarchy Level</b>	[edit services flow-collector transfer-log-archive archive-sites]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the username for the transfer log server.
<b>Options</b>	<i>username</i> —FTP server username.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Transfer Logs on page 1299</a></li> </ul>

## variant

---

<b>Syntax</b>	<pre>variant <i>variant-number</i> {   data-format <i>format</i>;   name-format <i>format</i>;   transfer {     record-level <i>number</i>;     timeout <i>seconds</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit services flow-collector file-specification]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure a variant of the file format.
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring File Formats on page 1298</a></li> </ul>



# Dynamic Flow Capture Configuration Guidelines

Dynamic flow capture enables you to capture packet flows on the basis of dynamic filtering criteria. Specifically, you can use this feature to forward passively monitored packet flows that match a particular filter list to one or more destinations using an on-demand control protocol.

This chapter contains the following sections:

- [Understanding Junos Capture Vision on page 1327](#)
- [Configuring Junos Capture Vision on page 1329](#)
- [Example: Configuring Junos Capture Vision on page 1335](#)

## Understanding Junos Capture Vision

---

Junos Capture Vision (known as dynamic flow capture in Junos OS Releases earlier than 13.2) enables you to capture packet flows on the basis of dynamic filtering criteria. Specifically, you can use this feature to forward passively monitored packet flows that match a particular filter list to one or more destinations using an on-demand control protocol.

This topic contains the following sections:

- [Junos Capture Vision Architecture on page 1327](#)
- [Liberal Sequence Windowing on page 1328](#)
- [Intercepting IPv6 Flows on page 1329](#)

## Junos Capture Vision Architecture

The architecture consists of one or more *control sources* that send requests to a Juniper Networks router to monitor incoming data, and then forward any packets that match specific filter criteria to a set of one or more *content destinations*. The architectural components are defined as follows:

- **Control source**—A client that monitors electronic data or voice transfer over the network. The control source sends filter requests to the Juniper Networks router using the Dynamic Task Control Protocol (DTCP), specified in draft-cavuto-dtcp-03.txt at

<http://www.ietf.org/internet-drafts>. The control source is identified by a unique identifier and an optional list of IP addresses.

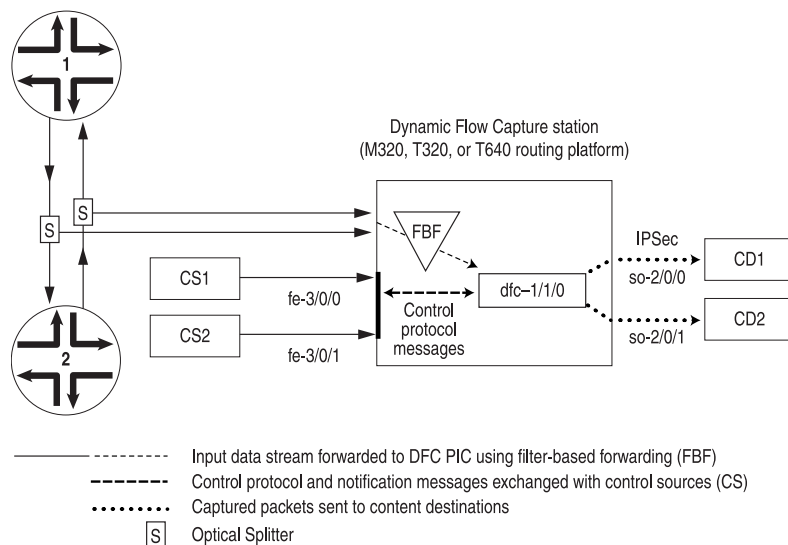
- Monitoring platform—A T Series or M320 router containing one or more Dynamic Flow Capture (DFC) PICs, which support dynamic flow capture processing. The monitoring platform processes the requests from the control sources, creates the filters, monitors incoming data flows, and sends the matched packets to the appropriate content destinations.
- Content destination—Recipient of the matched packets from the monitoring platform. Typically the matched packets are sent using an IPsec (IPsec) tunnel from the monitoring platform to another router connected to the content destination. The content destination and the control source can be physically located on the same host. For more information on IPsec tunnels, see *Junos VPN Site Secure*.



**NOTE:** The Junos Capture Vision PIC (either a Monitoring Services III PIC or Multiservices 400 PIC) forwards the entire packet content to the content destination, rather than to a content record as is done with cflowd or flow aggregation version 9 templates.

Figure 24 on page 1328 shows a sample topology. The number of control sources and content destinations is arbitrary.

Figure 24: Junos Capture Vision Topology



g0170/5

## Liberal Sequence Windowing

Each DTCP packet (add, delete, list, and refresh packets) contains a 64-bit sequence number to identify the order of the packets. Because the network is connectionless, the DTCP packets can arrive out of order to the router running the Junos Capture Vision application.

The *liberal sequence window* feature implements a negative window for the sequence numbers received in the DTCP packets. It enables the Junos Capture Vision application to accept not only DTCP packets with sequence numbers greater than those previously received, but also DTCP packets with lesser sequence numbers, up to a certain limit. This limit is the negative window size; the positive and negative window sizes are +256 and -256 respectively, relative to the current maximum sequence number received. No configuration is required to activate this feature; the window sizes are hard-coded and nonconfigurable.

## Intercepting IPv6 Flows

Starting with Junos OS Release 11.4, Junos Capture Vision also supports intercepting IPv6 flows in M320, T320, T640, and T1600 routers with a Multiservices 400 or Multiservices 500 PIC. Junos Capture Vision can intercept passively monitored IPv6 traffic only. All support for IPv4 interception remains the same. The interception of IPv6 traffic happens in the same way the filters capture IPv4 flows. With the introduction of IPv6 interception, both IPv4 and IPv6 filters can coexist. The mediation device, however, cannot be located in an IPv6 network.

Junos Capture Vision does not support interception of VPLS and MPLS traffic. The application cannot intercept Address Resolution Protocol (ARP) or other Layer 2 exception packets. The interception filter can be configured to timeout based on factors like total time (seconds), idle time (seconds), total packets or total data transmitted (bytes).

### Related Documentation

- [Configuring Junos Capture Vision on page 1329](#)
- [Example: Configuring Junos Capture Vision on page 1335](#)

---

## Configuring Junos Capture Vision

This section describes the following tasks for configuring Junos Capture Vision:

- [Configuring the Capture Group on page 1329](#)
- [Configuring the Content Destination on page 1330](#)
- [Configuring the Control Source on page 1331](#)
- [Configuring the DFC PIC Interface on page 1332](#)
- [Configuring the Firewall Filter on page 1333](#)
- [Configuring System Logging on page 1333](#)
- [Configuring Tracing Options for Junos Capture Vision Events on page 1334](#)
- [Configuring Thresholds on page 1334](#)
- [Limiting the Number of Duplicates of a Packet on page 1335](#)

### Configuring the Capture Group

A capture group defines a profile of Junos Capture Vision configuration information. The static configuration includes information about control sources, content destinations, and notification destinations. Dynamic configuration is added through interaction with control sources using a control protocol.

To configure a capture group, include the **capture-group** statement at the **[edit services dynamic-flow-capture]** hierarchy level:

```
capture-group client-name {  
  content-destination identifier {  
    address address;  
    hard-limit bandwidth;  
    hard-limit-target bandwidth;  
    soft-limit bandwidth;  
    soft-limit-clear bandwidth;  
    ttl hops;  
  }  
  control-source identifier {  
    allowed-destinations [ destinations ];  
    minimum-priority value;  
    no-syslog;  
    notification-targets address port port-number;  
    service-port port-number;  
    shared-key value;  
    source-addresses [ addresses ];  
  }  
  duplicates-dropped-periodicity seconds;  
  input-packet-rate-threshold rate;  
  interfaces interface-name;  
  max-duplicates number;  
  pic-memory-threshold percentage percentage;  
}
```

To specify the **capture-group**, assign it a unique **client-name** that associates the information with the requesting control sources.

## Configuring the Content Destination

You must specify a destination for the packets that match DFC PIC filter criteria. To configure the content destination, include the **content-destination** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

```
content-destination identifier {  
  address address;  
  hard-limit bandwidth;  
  hard-limit-target bandwidth;  
  soft-limit bandwidth;  
  soft-limit-clear bandwidth;  
  ttl hops;  
}
```

Assign the **content-destination** a unique **identifier**. You must also specify its IP address and you can optionally include additional settings:

- **address**—The DFC PIC interface appends an IP header with this destination address on the matched packet (with its own IP header and contents intact) and sends it out to the content destination.
- **ttl**—The time-to-live (TTL) value for the IP-IP header. By default, the TTL value is 255. Its range is 0 through 255.

- Congestion thresholds—You can specify per-content destination bandwidth limits that control the amount of traffic produced by the DFC PIC during periods of congestion. The thresholds are arranged in two pairs: **hard-limit** and **hard-limit-target**, and **soft-limit** and **soft-limit-clear**. You can optionally include one or both of these paired settings. All four settings are 10-second average bandwidth values in bits per second. Typically **soft-limit-clear** < **soft-limit** < **hard-limit-target** < **hard-limit**. When the content bandwidth exceeds the **soft-limit** setting:
  1. A congestion notification message is sent to each control source of the criteria that point to this content destination
  2. If the control source is configured for **syslog**, a system log message is generated.
  3. A latch is set, indicating that the control sources have been notified. No additional notification messages are sent until the latch is cleared, when the bandwidth falls below the **soft-limit-clear** value.

When the bandwidth exceeds the **hard-limit** value:

1. Junos Capture Vision begins deleting criteria until the bandwidth falls below the **hard-limit-target** value.
2. For each criterion deleted, a CongestionDelete notification is sent to the control source for that criterion.
3. If the control source is configured for **syslog**, a log message is generated.

The application evaluates criteria for deletion using the following data:

- Priority—Lower priority criteria are purged first, after adjusting for control source minimum priority.
- Bandwidth—Higher bandwidth criteria are purged first.
- Timestamp—The more recent criteria are purged first.

## Configuring the Control Source

You configure information about the control source, including allowed source addresses and destinations and authentication key values. To configure the control source information, include the **control-source** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

```
control-source identifier {
  allowed-destinations [ destination-identifiers ];
  minimum-priority value;
  no-syslog;
  notification-targets address port port-number;
  service-port port-number;
  shared-key value;
  source-addresses [ addresses ];
}
```

Assign the **control-source** statement a unique ***identifier***. You can also include values for the following statements:

- **allowed-destinations**—One or more content destination identifiers to which this control source can request that matched data be sent in its control protocol requests. If you do not specify any content destinations, all available destinations are allowed.
- **minimum-priority**—Value assigned to the control source that is added to the priority of the criteria in the DTCP ADD request to determine the total priority for the criteria. The lower the value, the higher the priority. By default, **minimum-priority** has a value of 0 and the allowed range is 0 through 254.
- **notification-targets**—One or more destinations to which the DFC PIC interface can log information about control protocol-related events and other events such as PIC bootup messages. You configure each **notification-target** entry with an IP **address** value and a User Datagram Protocol (UDP) **port** number.
- **service-port**—UDP port number to which the control protocol requests are directed. Control protocol requests that are not directed to this port are discarded by DFC PIC interfaces.
- **shared-key**—20-byte authentication key value shared between the control source and the DFC PIC monitoring platform.
- **source-addresses**—One or more allowed IP addresses from which the control source can send control protocol requests to the DFC PIC monitoring platform. These are /32 addresses.

## Configuring the DFC PIC Interface

You specify the interface that interacts with the control sources configured in the same capture group. A Monitoring Services III PIC can belong to only one capture group, and you can configure only one PIC for each group.

To configure a DFC PIC interface, include the **interfaces** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

```
interfaces interface-name;
```

You specify DFC interfaces using the **dfc-** identifier at the **[edit interfaces]** hierarchy level. You must specify three logical units on each DFC PIC interface, numbered 0, 1, and 2. You cannot configure any other logical interfaces.

- **unit 0** processes control protocol requests and responses.
- **unit 1** receives monitored data.
- **unit 2** transmits the matched packets to the destination address.

The following example shows the configuration necessary to set up a DFC PIC interface and intercept both IPv4 and IPv6 traffic:

```
[edit interfaces dfc-0/0/0]
unit 0 {
  family inet {
    filter {
      output high; #Firewall filter to route control packets
      # through 'network-control' forwarding class. Control packets
```

```

        # are loss sensitive.
    }
    address 10.1.0.0/32 { # DFC PIC address
        destination 10.36.100.1; # DFC PIC address used by
        # the control source to correspond with the
        # monitoring platform
    }
}
unit 1 { # receive data packets on this logical interface
    family inet; # receive IPv4 traffic for interception
    family inet6; # receive IPv6 traffic for interception
}
unit 2 { # send out copies of matched packets on this logical interface
    family inet;
}

```

In addition, you must configure Junos Capture Vision to run on the DFC PIC in the correct chassis location. The following example shows this configuration at the **[edit chassis]** hierarchy level:

```

fpc 0 {
    pic 0 {
        monitoring-services application dynamic-flow-capture;
    }
}

```

For more information on configuring chassis properties, see the *Junos OS Administration Library for Routing Devices*.

## Configuring the Firewall Filter

You can specify the firewall filter to route control packets through the network control forwarding class. The control packets are loss sensitive. To configure the firewall filter, include the following statements at the **[edit]** hierarchy level:

```

firewall {
    family inet {
        filter high {
            term all {
                then forwarding-class network-control;
            }
        }
    }
}

```

## Configuring System Logging

By default, control protocol activity is logged as a separate system log facility, **dfc**. To modify the filename or level at which control protocol activity is recorded, include the following statements at the **[edit syslog]** hierarchy level:

```

file dfc.log {
    dfc any;
}

```

To cancel logging, include the **no-syslog** statement at the **[edit services dynamic-flow-capture capture-group *client-name* control-source *identifier*]** hierarchy level:

**no-syslog;**



**NOTE:** Junos Capture Vision (dfc-) interface supports up to 10,000 filter criteria. When more than 10,000 filters are added to the interface, the filters are accepted, but system log messages are generated indicating that the filter is full.

---

## Configuring Tracing Options for Junos Capture Vision Events

You can enable tracing options for Junos Capture Vision events by including the **traceoptions** statement at the **[edit services dynamic-flow-capture]** hierarchy level.

When you include the **traceoptions** configuration, you can also specify the trace file name, maximum number of trace files, the maximum size of trace files, and whether the trace file can be read by all users or not.

To enable tracing options for Junos Capture Vision events, include the following configuration at the **[edit services dynamic-flow-capture]** hierarchy level:

```
traceoptions{
  file filename <files number> <size size> <world-readable | non-world-readable>;
}
```

To disable tracing for Junos Capture Vision events, delete the **traceoptions** configuration from the **[edit services dynamic-flow-capture]** hierarchy level.



**NOTE:** In Junos OS releases earlier than 9.2R1, tracing of Junos Capture Vision was enabled by default, and the logs were saved to the **/var/log/dfcd** directory.

---

## Configuring Thresholds

You can optionally specify threshold values for the following situations in which warning messages will be recorded in the system log:

- Input packet rate to the DFC PIC interfaces
- Memory usage on the DFC PIC interfaces

To configure threshold values, include the **input-packet-rate-threshold** or **pic-memory-threshold** statements at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

```
input-packet-rate-threshold rate;  
pic-memory-threshold percentage percentage;
```

If these statements are not configured, no threshold messages are logged. The threshold settings are configured for the capture group as a whole.

The range of configurable values for the **input-packet-rate-threshold** statement is 0 through 1 Mpps. The PIC calibrates the value accordingly; the Monitoring Services III PIC caps the threshold value at 300 Kpps and the Multiservices 400 PIC uses the full configured value. The range of values for the **pic-memory-threshold** statement is 0 to 100 percent.

## Limiting the Number of Duplicates of a Packet

You can optionally specify the maximum number of duplicate packets the DFC PIC is allowed to generate from a single input packet. This limitation is intended to reduce the load on the PIC when packets are sent to multiple destinations. When the maximum number is reached, the duplicates are sent to the destinations with the highest criteria class priority. Within classes of equal priority, criteria having earlier timestamps are selected first.

To configure this limitation, include the **max-duplicates** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level:

```
max-duplicates number;
```

You can also apply the limitation on a global basis for the DFC PIC by including the **g-max-duplicates** statement at the **[edit services dynamic-flow-capture]** hierarchy level:

```
g-max-duplicates number;
```

By default, the maximum number of duplicates is set to 3. The range of allowed values is 1 through 64. A setting for **max-duplicates** for an individual capture-group overrides the global setting.

In addition, you can specify the frequency with which the application sends notifications to the affected control sources that duplicates are being dropped because the threshold has been reached. You configure this setting at the same levels as the maximum duplicates settings, by including the **duplicates-dropped-periodicity** statement at the **[edit services dynamic-flow-capture capture-group *client-name*]** hierarchy level or the **g-duplicates-dropped-periodicity** statement at the **[edit services dynamic-flow-capture]** hierarchy level:

```
duplicates-dropped-periodicity seconds;  
g-duplicates-dropped-periodicity seconds;
```

As with the **g-max-duplicates** statement, the **g-duplicates-dropped-periodicity** statement applies the setting globally for the application and is overridden by a setting applied at the capture-group level. By default, the frequency for sending notifications is 30 seconds.

### Related Documentation

- [Understanding Junos Capture Vision on page 1327](#)
- [Example: Configuring Junos Capture Vision on page 1335](#)

## Example: Configuring Junos Capture Vision

The following example includes all parts of a complete Junos Capture Vision configuration.

Configure the Junos Capture Vision PIC interface:

```
[edit interfaces dfc-0/0/0]
unit 0 {
  family inet {
    filter {
      output high; #Firewall filter to route control packets
      # through 'network-control' forwarding class. Control packets
      # are loss sensitive.
    }
    address 10.1.0.0/32 { # DFC PIC address
      destination 10.36.100.1; # DFC PIC address used by
      # the control source to correspond with the
      # monitoring platform
    }
  }
}
unit 1 { # receive data packets on this logical interface
  family inet;
  family inet6;
}
unit 2 { # send out copies of matched packets on this logical interface
  family inet;
}
```

Configure the capture group:

```
services dynamic-flow-capture {
  capture-group g1 {
    interfaces dfc-0/0/0;
    input-packet-rate-threshold 90k;
    pic-memory-threshold percentage 80;
    control-source cs1 {
      source-addresses 10.36.41.1;
      service-port 2400;
      notification-targets {
        10.36.41.1 port 2100;
      }
      shared-key "$9$ASxdsYoX7wg4aHk";
      allowed-destinations cd1;
    }
    content-destination cd1 {
      address 10.36.70.2;
      ttl 244;
    }
  }
}
```

Configure filter-based forwarding (FBF) to the Junos Capture Vision PIC interface, logical unit 1.

For more information about configuring passive monitoring interfaces, see [“Enabling Passive Flow Monitoring” on page 1203](#).

```
interfaces so-1/2/0 {
  encapsulation ppp;
  unit 0 {
    passive-monitor-mode;
```

```

    family inet {
        filter {
            input catch;
        }
    }
}

```

Configure the firewall filter:

```

firewall {
    filter catch {
        interface-specific;
        term def {
            then {
                count counter;
                routing-instance fbf_inst;
            }
        }
    }
    family inet {
        filter high {
            term all {
                then forwarding-class network-control;
            }
        }
    }
}

```

Configure a forwarding routing instance. The next hop points specifically to the logical interface corresponding to **unit 1**, because only this particular logical unit is expected to relay monitored data to the Junos Capture Vision PIC.

```

routing-instances fbf_inst {
    instance-type forwarding;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop dfc-0/0/0.1;
        }
    }
}

```

Configure routing table groups:

```

[edit]
routing-options {
    interface-routes {
        rib-group inet common;
    }
    rib-groups {
        common {
            import-rib [ inet.0 fbf_inst.inet.0 ];
        }
    }
    forwarding-table {
        export pplb;
    }
}

```

```
}
```

Configure interfaces to the control source and content destination:

```
interfaces fe-4/1/2 {  
  description "to cs1 from dfc";  
  unit 0 {  
    family inet {  
      address 10.36.41.2/30;  
    }  
  }  
}  
interfaces ge-7/0/0 {  
  description "to cd1 from dfc";  
  unit 0 {  
    family inet {  
      address 10.36.70.1/30;  
    }  
  }  
}
```

**Related  
Documentation**

- [Understanding Junos Capture Vision on page 1327](#)
- [Configuring Junos Capture Vision on page 1329](#)

# Flow-Tap Configuration Guidelines

Dynamic flow capture enables you to capture packet flows on the basis of dynamic filtering criteria, using Dynamic Tasking Control Protocol (DTCP) requests. The flow-tap application extends the use of this protocol to intercept IPv4 and IPv6 packets in an active monitoring router and send a copy of packets that match filter criteria to one or more content destinations. Flow-tap data can be used in the following applications:

- Flexible trend analysis for detection of new security threats
- Lawful intercept

Flow-tap service is supported on M Series and T Series routers, except M160 and TX Matrix routers. Flow-tap filters are applied on all IPv4 traffic and do not add any perceptible delay in the forwarding path. Flow-tap filters can also be applied on IPv6 traffic. For security, filters installed by one client are not visible to others and the CLI configuration does not reveal the identity of the monitored target. A lighter version of the application is supported on MX Series routers only; for more information, see “[Configuring FlowTapLite](#)” on page 1344.



**NOTE:** For information about dynamic flow capture, see “[Dynamic Flow Capture Configuration Guidelines](#)” on page 1327. For information about DTCP, see [draft-cavuto-dtcp-01.txt](#) at <http://www.ietf.org/internet-drafts>.

To configure flow-tap services, include the **flow-tap** statement at the **[edit services]** hierarchy level. You can also specify whether you want to apply the flow-tap service to IPv4 traffic or IPv6 traffic by including the **family inet | inet6** statement. If the **family** statement is not included in the configuration, the flow-tap service is applied only to the IPv4 traffic.

```
flow-tap {  
  interface interface-name;  
  family inet | inet6;  
}
```

Other statements are configured at the **[edit interfaces]** and **[edit system]** hierarchy levels.

This chapter contains the following sections:

- [Junos Packet Vision Architecture on page 1340](#)
- [Configuring Junos Packet Vision on page 1342](#)
- [Configuring FlowTapLite on page 1344](#)
- [Examples: Configuring Junos Packet Vision on page 1346](#)

---

## Junos Packet Vision Architecture

The Junos Packet Vision (previously known as Flow-Tap) architecture consists of one or more *mediation devices* that send requests to a Juniper Networks router to monitor incoming data and forward any packets that match specific filter criteria to a set of one or more *content destinations*:

- **Mediation device**—A client that monitors electronic data or voice transfer over the network. The mediation device sends filter requests to the Juniper Networks router using the DTCP. The clients are not identified for security reasons, but have permissions defined by a set of special login classes. Each system can support up to 16 different mediation devices for each user, up to a maximum of 64 mediation devices for the whole system.
- **Monitoring platform**—An M Series or T Series router containing one or more Adaptive Services (AS) or Multiservices PICs, which are configured to support the Junos Packet Vision application. The monitoring platform processes the requests from the mediation devices, applies the dynamic filters, monitors incoming data flows, and sends the matched packets to the appropriate content destinations.
- **Content destination**—Recipient of the matched packets from the monitoring platform. Typically the matched packets are sent using an IP Security (IPsec) tunnel from the monitoring platform to another router connected to the content destination. The content destination and the mediation device can be physically located on the same host. For more information about IPsec tunnels, see *Junos VPN Site Secure*.
- **Dynamic filters**—Firewall filters automatically generated by the Packet Forwarding Engine and applied to all routing instances. Each term in the filter includes a **flow-tap** action that is similar to the existing **sample** or **port-mirroring** actions. As long as one of the filter terms matches an incoming packet, the router copies the packet and forwards it to the Adaptive Services or Multiservices PIC that is configured for Junos Packet Vision service. The Adaptive Services or Multiservices PIC runs the packet through the client filters and sends a copy to each matching content destination.

Following is a sample filter configuration; note that it is dynamically generated by the router (no user configuration is required):

```
filter combined_LEA_filter {
  term LEA1_filter {
    from {
      source-address 1.2.3.4;
      destination-address 3.4.5.6;
    }
    then {
      flow-tap;
    }
  }
}
```

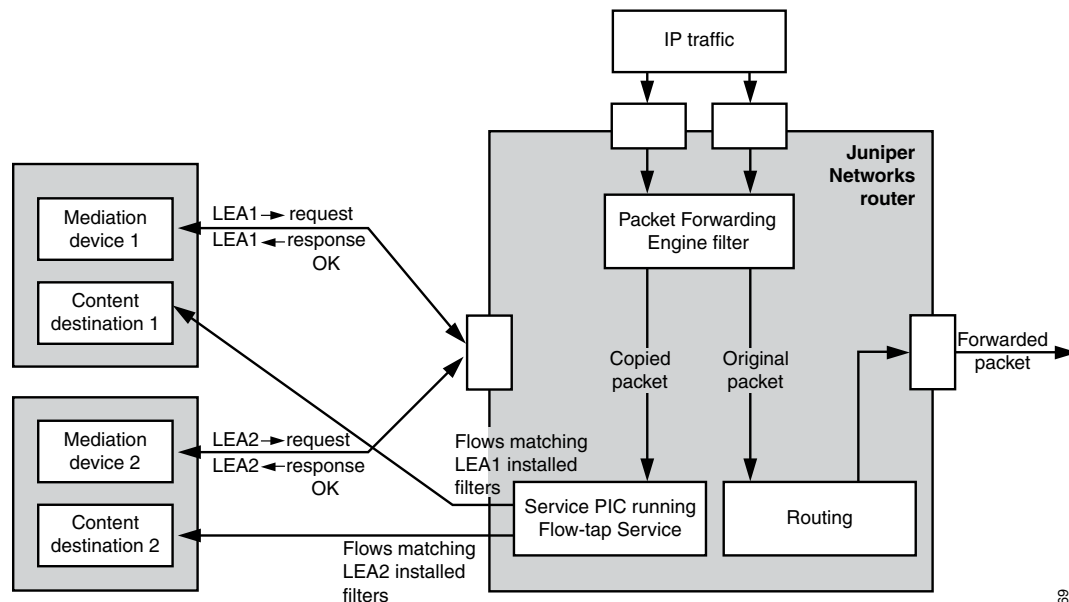
```

    }
  }
  term LEA2_filter {
    from {
      source-address 10.1.1.1;
      source-port 23;
    }
    then {
      flow-tap;
    }
  }
}

```

Figure 25 on page 1341 shows a sample topology that uses two mediation devices and two content destinations.

Figure 25: Junos Packet Vision Topology



LEA = Law Enforcing Authority

#### Related Documentation

- [Understanding Junos Packet Vision](#)
- [\[edit services flow-tap\] Hierarchy Level](#)
- [Configuring Junos Packet Vision on page 1342](#)
- [Examples: Configuring Junos Packet Vision on page 1346](#)

## Configuring Junos Packet Vision

---

This topic explains Junos Packet Vision (previously known as Flow-Tap) configuration, and contains the following sections:

- [Configuring the Junos Packet Vision Interface on page 1342](#)
- [Strengthening Junos Packet Vision Security on page 1342](#)
- [Restrictions on Junos Packet Vision Services on page 1343](#)

### Configuring the Junos Packet Vision Interface

To configure an adaptive services interface for flow-tap service, include the **interface** statement at the **[edit services flow-tap]** hierarchy level:

```
interface sp-fpc/pic/port.unit-number;
```

You can assign any Adaptive Services or Multiservices PIC in the active monitoring router for Junos Packet Vision, and use any logical unit on the PIC.

You can specify the type of traffic for which you want to apply the Junos Packet Vision service by including the **family inet | inet6** statement. If the **family** statement is not included, the Junos Packet Vision service is, by default, applied to the IPv4 traffic. To apply Junos Packet Vision service to IPv6 traffic, you must include the **family inet6** statement in the configuration. To enable the Junos Packet Vision service for IPv4 and IPv6 traffic, you must explicitly configure the **family** statement for both **inet** and **inet6** families.



**NOTE:** You cannot configure Junos Capture Vision (previously known as dynamic flow capture) and Junos Packet Vision services on the same router simultaneously.

You must also configure the logical interface at the **[edit interfaces]** hierarchy level:

```
interface sp-fpc/pic/port {  
  unit logical-unit-number {  
    family inet;  
    family inet6;  
  }  
}
```



**NOTE:** If you do not include the **family inet6** statement in the configuration, IPv6 flows will not be intercepted.

### Strengthening Junos Packet Vision Security

You can add an extra level of security to Dynamic Tasking Control Protocol (DTCP) transactions between the mediation device and the router by enabling DTCP sessions on top of the SSH layer. To configure SSH settings, include the **flow-tap-dtcp** statement at the **[edit system services]** hierarchy level:

```

flow-tap-dtcp {
  ssh {
    connection-limit value;
    rate-limit value;
  }
}

```

To configure client permissions for viewing and modifying Junos Packet Vision configurations and for receiving tapped traffic, include the **permissions** statement at the **[edit system login class class-name]** hierarchy level:

```
permissions [permissions];
```

The permissions needed to use Junos Packet Vision features are as follows:

- **flow-tap**—Can view Junos Packet Vision configuration
- **flow-tap-control**—Can modify Junos Packet Vision configuration
- **flow-tap-operation**—Can tap flows

You can also specify user permissions on a RADIUS server, for example:

```

Bob Auth-Type := Local, User-Password = "abc123"
Juniper-User-Permissions = "flow-tap-operation"

```

For details on **[edit system]** and RADIUS configuration, see the *Junos OS Administration Library for Routing Devices*.

## Restrictions on Junos Packet Vision Services

The following restrictions apply to Junos Packet Vision services:

- You cannot configure Junos Capture Vision and Junos Packet Vision features on the same router simultaneously.
- On routers that support LMNR-based FPCs, you cannot configure the Junos Packet Vision for IPv6 along with port mirroring or sampling of IPv6 traffic. This restriction applies even if the router does not have any LMNR-based FPC installed in it. However, there is no restriction on configuring Junos Packet Vision on routers that are configured for port mirroring or sampling of IPv4 traffic.
- Junos Packet Vision does not support interception of MPLS and virtual private LAN service (VPLS).
- Junos Packet Vision cannot intercept Address Resolution Protocol (ARP) and other Layer 2 exceptions.
- IPv4 and IPv6 intercept filters can coexist on a system, subject to a combined maximum of 100 filters.
- When Junos Capture Vision process or the Adaptive Services or Multiservices PIC configured for Junos Packet Vision restarts, all filters are deleted and the mediation devices are disconnected.
- Only the first fragment of an IPv4 fragmented packet stream is sent to the content destination.

- Port mirroring might not work in conjunction with Junos Packet Vision.
- Running the Junos Packet Vision over an IPsec tunnel on the same router can cause packet loops and is not supported.
- M10i routers do not support the standard Junos Packet Vision, but do support FlowTapLite (see [“Configuring FlowTapLite” on page 1344](#)). Junos Packet Vision and FlowTapLite cannot be configured simultaneously on the same chassis.
- PIC-based flow-tap is not supported on M7i and M10i routers equipped with an Enhanced Compact Forwarding Engine Board (CFEB-E).
- You cannot configure Junos Packet Vision on channelized interfaces.

**Related  
Documentation**

- [Configuring FlowTapLite on page 1344](#)

---

## Configuring FlowTapLite

A lighter version of the flow-tap application is available on MX Series routers and also on M320 routers with Enhanced III Flexible PIC Concentrators (FPCs). All of the functionality resides in the Packet Forwarding Engine rather than a service PIC or Dense Port Concentrator (DPC).



**NOTE:** On M320 routers only, if the replacement of FPCs results in a mode change, you must restart the dynamic flow capture process manually by disabling and then re-enabling the CLI configuration.

FlowTapLite uses the same DTCP-SSH architecture to install the Dynamic Tasking Control Protocol (DTCP) filters and authenticate the users as the original flow-tap application and supports up to 3000 filters per chassis.



**NOTE:** The original flow-tap application and FlowTapLite cannot be used at the same time.

To configure FlowTapLite, include the **flow-tap** statement at the **[edit services]** hierarchy level:

```
flow-tap {  
    tunnel-interface interface-name;  
}
```

For the Packet Forwarding Engine to encapsulate the intercepted packet, it must send the packet to a tunnel logical (**vt-**) interface. You need to allocate a tunnel interface and assign it to the dynamic flow capture process for FlowTapLite to use. To create the tunnel interface, include the following configuration:

```
chassis {  
    fpc number {  
        pic number {
```

```

    tunnel-services {
        bandwidth (1g | 10g);
    }
}
}

```



**NOTE:** Currently FlowTapLite supports only one tunnel interface per instance.

For more information about this configuration, see the *Junos OS Administration Library for Routing Devices*.

To configure the logical interfaces and assign them to the dynamic flow capture process, include the following configuration:

```

interfaces {
    vt-fpc/pic/port {
        unit 0 {
            family inet;
            family inet6;
        }
    }
}

```



**NOTE:** If a service PIC or DPC is available, you can use its tunnel interface for the same purpose.



**NOTE:** If you do not include the `family inet6` statement in the configuration, IPv6 flows will not be intercepted.



**NOTE:** With FlowTapLite configured and traceoptions enabled, if you add more than two content destinations by including the X-JTAP-CDEST-DEST-ADDRESS line in the Dynamic Tasking Control Protocol (DTCP) parameter file and initiate a DTCP session by sending a DTCP ADD message, a '400 BAD request' message is received. Although you can specify more than two content destinations in the DTCP file that is sent from the mediation device, this error message occurs when the DTCP ADD message is sent. This behavior is expected with more than two content destinations. You must specify only two content destinations per DTCP ADD message.

#### Related Documentation

- [Understanding Junos Packet Vision](#)
- [\[edit services flow-tap\] Hierarchy Level](#)
- [Configuring Junos Packet Vision on page 1342](#)
- [Examples: Configuring Junos Packet Vision on page 1346](#)

## Examples: Configuring Junos Packet Vision

---

The following example shows all parts of a complete Junos Packet Vision configuration with IPv4 and IPv6 flow intercepts

```
services {
  flow-tap {
    interface sp-1/2/0.100;
  }
}
interfaces {
  sp-1/2/0 {
    unit 100 {
      family inet;
      family inet6;
    }
  }
}
system {
  services {
    flow-tap-dtcp {
      ssh {
        connection-limit 5;
        rate-limit 5;
      }
    }
  }
  login {
    class ft-class {
      permissions flow-tap-operation;
    }
    user ft-user1 {
      class ft-class;
      authentication {
        encrypted-password "xxxx";
      }
    }
  }
}
```

The following example shows a FlowTapLite configuration that intercepts IPv4 and IPv6 flows:

```
system {
  login {
    class flowtap {
      permissions flow-tap-operation;
    }
    user ftap {
      uid 2000;
      class flowtap;
      authentication {
        encrypted-password "$1$nZfwNn4L$TWi/oxFwFZyOyyxN/87Jv0"; ##
        SECRET-DATA
      }
    }
  }
}
```

```

    }
  }
  services {
    flow-tap-dtcp {
      ssh;
    }
  }
}
chassis {
  fpc 0 {
    pic 0 {
      tunnel-services {
        bandwidth 10g;
      }
    }
  }
}
interfaces {
  vt-0/0/0 {
    unit 0 {
      family inet;
      family inet6;
    }
  }
}
services {
  flow-tap {
    tunnel-interface vt-0/0/0.0;
  }
}

```

#### Related Documentation

- [Understanding Junos Packet Vision](#)
- [\[edit services flow-tap\] Hierarchy Level](#)
- [Configuring Junos Packet Vision on page 1342](#)
- [Configuring FlowTapLite on page 1344](#)



## CHAPTER 56

# Summary of Dynamic Flow Capture and Flow-Tap Configuration Statements

The following sections explain each of the dynamic flow capture and flow-tap configuration statements. The statements are organized alphabetically.

### address (Services Dynamic Flow Capture)

---

<b>Syntax</b>	<code>address <i>address</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services dynamic-flow-capture <i>capture-group</i> <i>client-name</i> <i>content-destination</i> <i>identifier</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Configure an IP address for the flow capture destination.
<b>Options</b>	<i>address</i> —IP address for the content destination.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Content Destination on page 1330</a></li></ul>

## allowed-destinations

---

<b>Syntax</b>	<code>allowed-destinations [ <i>identifiers</i> ];</code>
<b>Hierarchy Level</b>	<code>[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> <a href="#">control-source</a> <i>identifier</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Identify flow capture destinations that are allowed in messages sent from this control source.
<b>Options</b>	<i>identifier</i> —Allowed content destination name.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Control Source on page 1331</a></li></ul>

## capture-group

<b>Syntax</b>	<pre>capture-group <i>client-name</i> {   content-destination <i>identifier</i> {     address <i>address</i>;     hard-limit <i>bandwidth</i>;     hard-limit-target <i>bandwidth</i>;     soft-limit <i>bandwidth</i>;     soft-limit-clear <i>bandwidth</i>;     ttl <i>hops</i>;   }   control-source <i>identifier</i> {     allowed-destinations [ <i>destinations</i> ];     minimum-priority <i>value</i>;     no-syslog;     notification-targets <i>address</i> port <i>port-number</i>;     service-port <i>port-number</i>;     shared-key <i>value</i>;     source-addresses [ <i>addresses</i> ];   }   duplicates-dropped-periodicity <i>seconds</i>;   input-packet-rate-threshold <i>rate</i>;   interfaces <i>interface-name</i>;   max-duplicates <i>number</i>;   pic-memory-threshold <i>percentage percentage</i>; }</pre>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Define the capture group values.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Capture Group on page 1329</a></li> </ul>

## content-destination

---

<b>Syntax</b>	<pre>content-destination <i>identifier</i> {     address (Services Dynamic Flow Capture) <i>address</i>;     hard-limit <i>bandwidth</i>;     hard-limit-target <i>bandwidth</i>;     soft-limit <i>bandwidth</i>;     soft-limit-clear <i>bandwidth</i>;     ttl <i>hops</i>; }</pre>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <b>capture-group</b> <i>client-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Identify the destination for captured packets.
<b>Options</b>	<p><i>identifier</i>—Name of the destination.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Content Destination on page 1330</a></li></ul>

## control-source

---

Syntax	<pre>control-source <i>identifier</i> {     allowed-destinations [ <i>destinations</i> ];     minimum-priority <i>value</i>;     no-syslog;     notification-targets <i>address</i> port <i>port-number</i>;     service-port <i>port-number</i>;     shared-key <i>value</i>;     source-addresses [ <i>addresses</i> ]; }</pre>
Hierarchy Level	[edit services dynamic-flow-capture <b>capture-group</b> <i>client-name</i> ]
Release Information	Statement introduced in Junos OS Release 7.4.
Description	Identify the source of the dynamic flow capture request.
Options	<p><i>identifier</i>—Name of control source.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Control Source on page 1331</a></li></ul>

## **duplicates-dropped-periodicity**

---

<b>Syntax</b>	<code>duplicates-dropped-periodicity <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the frequency for sending notifications to affected control sources when transmission of duplicate sets of data is restricted because the <b>max-duplicates</b> threshold has been reached.
<b>Options</b>	<b>seconds</b> —Period for sending DuplicatesDropped notifications. <b>Default:</b> 30 seconds
<b>Usage Guidelines</b>	See .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">g-duplicates-dropped-periodicity on page 1357</a></li><li>• <a href="#">Limiting the Number of Duplicates of a Packet on page 1335</a></li><li>• <a href="#">max-duplicates on page 1361</a></li></ul>

## dynamic-flow-capture

```
Syntax  dynamic-flow-capture {
        capture-group client-name {
            content-destination identifier {
                address address;
                hard-limit bandwidth;
                hard-limit-target bandwidth;
                soft-limit bandwidth;
                soft-limit-clear bandwidth;
                ttl hops;
            }
            control-source identifier {
                allowed-destinations [ destinations ];
                minimum-priority value;
                no-syslog;
                notification-targets address port port-number;
                service-port port-number;
                shared-key value;
                source-addresses [ addresses ];
            }
            duplicates-dropped-periodicity seconds;
            input-packet-rate-threshold rate;
            interfaces interface-name;
            max-duplicates number;
            pic-memory-threshold percentage percentage;
        }
        g-duplicates-dropped-periodicity seconds;
        g-max-duplicates number;
    }
```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced in Junos OS Release 7.4.

**Description** Define the dynamic flow capture properties to be applied to traffic.

**Options** The remaining statements are explained separately.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Dynamic Flow Capture*

## flow-tap

---

<b>Syntax</b>	<pre>flow-tap {   (<b>interface</b> <i>interface-name</i>   tunnel-interface <i>interface-name</i>   family (inet   inet6)); }</pre>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Enable the flow-tap or FlowTapLite application on an interface. FlowTapLite is a lighter version of the flow-tap application that is available on MX Series platforms, M120 routers, and M320 routers with Enhanced III FPCs only.
<b>Options</b>	<p><b>interface <i>interface-name</i></b>—Specify the interface name for the flow-tap application.</p> <p><b>tunnel-interface <i>interface-name</i></b>—Specify the tunnel interface name for the FlowTapLite application.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>[edit services flow-tap] Hierarchy Level</i></li><li>• <a href="#">Configuring Junos Packet Vision on page 1342</a></li></ul>

## **g-duplicates-dropped-periodicity**

---

<b>Syntax</b>	<b>g-duplicates-dropped-periodicity</b> <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the frequency for sending notifications to affected control sources when transmission of duplicate sets of data is restricted because the <b>g-max-duplicates</b> threshold has been reached. This setting is applied globally; the <b>duplicates-dropped-periodicity</b> setting applied at the <b>capture-group</b> level overrides the global setting.
<b>Default</b>	The default period for sending notifications is 30 seconds.
<b>Options</b>	<i>seconds</i> —Period for sending DuplicatesDropped notifications.
<b>Usage Guidelines</b>	See .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">duplicates-dropped-periodicity on page 1354</a></li><li>• <a href="#">Limiting the Number of Duplicates of a Packet on page 1335</a></li></ul>

## g-max-duplicates

---

Syntax	<code>g-max-duplicates <i>number</i>;</code>
Hierarchy Level	[edit services dynamic-flow-capture]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Specify the maximum number of content destinations to which DFC PICs can send data from a single input set of packets. Limiting the number of duplicates reduces the load on the PIC. This setting is applied globally; the <b>max-duplicates</b> setting applied at the <b>capture-group</b> level overrides the global setting.
Default	If no value is configured, a default setting of 3 is used.
Options	<i>number</i> —Maximum number of content destinations. Range: 1 through 64
Usage Guidelines	See .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">max-duplicates on page 1361</a></li><li>• <a href="#">Limiting the Number of Duplicates of a Packet on page 1335</a></li></ul>

## hard-limit

---

Syntax	<code>hard-limit <i>bandwidth</i>;</code>
Hierarchy Level	[edit services dynamic-flow-capture capture-group <i>client-name</i> content-destination <i>identifier</i> ]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Specify a bandwidth threshold at which the dynamic flow capture application begins deleting criteria, until the bandwidth falls below the <b>hard-limit-target</b> value.
Options	<i>bandwidth</i> —Hard limit threshold, in bits per second.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">hard-limit-target on page 1359</a></li><li>• <a href="#">Configuring the Content Destination on page 1330</a></li></ul>

## hard-limit-target

---

<b>Syntax</b>	<code>hard-limit-target <i>bandwidth</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services dynamic-flow-capture capture-group <i>client-name</i> content-destination <i>identifier</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify a bandwidth threshold at which the dynamic flow capture application stops deleting criteria.
<b>Options</b>	<i>bandwidth</i> —Target value, in bits per second.
<b>Usage Guidelines</b>	See .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">hard-limit on page 1358</a></li><li>• <a href="#">Configuring the Content Destination on page 1330</a></li></ul>

## input-packet-rate-threshold

---

<b>Syntax</b>	<code>input-packet-rate-threshold <i>rate</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Specify a packet rate threshold value that triggers a system log warning message.
<b>Options</b>	<i>rate</i> —Threshold value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Thresholds on page 1334</a></li></ul>

## interface (Services Flow Tap)

---

<b>Syntax</b>	<code>interface sp-fpc/pic/port.logical-unit-number;</code>
<b>Hierarchy Level</b>	[edit services <a href="#">flow-tap</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1.
<b>Description</b>	Specify the AS PIC interface used with the flow-tap application. Any AS PIC available in the router can be assigned, and any logical interface on the AS PIC can be used.
<b>Options</b>	<b><i>interface-name</i></b> —Name of the DFC interface.  You cannot configure flow-tap services on channelized interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Junos Packet Vision Interface on page 1342</a></li></ul>

## interfaces (Services Dynamic Flow Capture)

---

<b>Syntax</b>	<code>interfaces interface-name;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Specify the DFC interface used with the control source configured in the same capture group.
<b>Options</b>	<b><i>interface-name</i></b> —Name of the DFC interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the DFC PIC Interface on page 1332</a></li></ul>

## max-duplicates

---

<b>Syntax</b>	<code>max-duplicates <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the maximum number of content destinations to which the DFC PIC can send data from a single input set of packets. Limiting the number of duplicates reduces the load on the PIC. This setting overrides the globally applied <b>g-max-duplicates</b> setting.
<b>Default</b>	If no value is configured, a default setting of 3 is used.
<b>Options</b>	<b><i>number</i></b> —Maximum number of content destinations. <b>Range:</b> 1 through 64
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">g-max-duplicates on page 1358</a></li><li>• <a href="#">Limiting the Number of Duplicates of a Packet on page 1335</a></li></ul>

## minimum-priority

---

<b>Syntax</b>	<code>minimum-priority <i>value</i>;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> <a href="#">control-source</a> <i>identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the minimum priority for the control source.
<b>Options</b>	<b><i>value</i></b> —Minimum priority value; if not specified, defaults to 0. <b>Range:</b> 0 through 254
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Control Source on page 1331</a></li></ul>

## no-syslog

---

<b>Syntax</b>	no-syslog;
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> <a href="#">control-source</a> <i>identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Disable system logging of control protocol requests and responses. By default, these messages are logged.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring System Logging on page 1333</a></li></ul>

## notification-targets

---

<b>Syntax</b>	notification-targets <i>address</i> <i>port port-number</i> ;
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> <a href="#">control-source</a> <i>identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	List of destination IP addresses and User Datagram Protocol (UDP) ports to which DFC PICs log exception information and control protocol state transitions, such as timeout values.
<b>Options</b>	<i>address address</i> —Allowed destination IP address.  <i>port port-number</i> —Allowed destination UDP port number.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Control Source on page 1331</a></li></ul>

## pic-memory-threshold

---

<b>Syntax</b>	<code>pic-memory-threshold percentage <i>percentage</i>;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Specify a PIC memory usage percentage that triggers a system log warning message.
<b>Options</b>	<i>percentage</i> —PIC memory threshold value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Thresholds on page 1334</a></li></ul>

## service-port

---

<b>Syntax</b>	<code>service-port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> <a href="#">control-source</a> <i>identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Identify the User Datagram Protocol (UDP) port number for control protocol requests.
<b>Options</b>	<i>port-number</i> —Port number for control protocol request messages.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Control Source on page 1331</a></li></ul>

## services (Dynamic Flow Capture)

---

<b>Syntax</b>	<code>services dynamic-flow-capture { ... },</code> <code>services flow-tap {...}</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	<b>dynamic-flow-capture</b> statement introduced in Junos OS Release 7.4. <b>flow-tap</b> statement introduced in Junos OS Release 8.1.
<b>Description</b>	Define the services to be applied to traffic.
<b>Options</b>	<b>dynamic-flow-capture</b> —The values configured for dynamic flow capture.  <b>flow-tap</b> —The values configured for the flow-tap application.  The statements are explained separately.
<b>Usage Guidelines</b>	See <a href="#">“Configuring Junos Capture Vision” on page 1329</a> or <a href="#">“Configuring Junos Packet Vision” on page 1342</a> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## shared-key

---

<b>Syntax</b>	<code>shared-key value;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> <a href="#">control-source</a> <i>identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Configure the authentication key value.
<b>Options</b>	<b>value</b> —Secret authentication value shared between a control source and destination.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Control Source on page 1331</a></li></ul>

## soft-limit

---

<b>Syntax</b>	<code>soft-limit <i>bandwidth</i>;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture capture-group <i>client-name</i> content-destination <i>identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify a bandwidth threshold at which congestion notifications are sent to each control source of the criteria that point to this content destination. If the control source is configured with the <b>syslog</b> statement, a log message will also be generated.
<b>Options</b>	<b><i>bandwidth</i></b> —Soft limit threshold, in bits per second.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Content Destination on page 1330</a></li></ul>

## soft-limit-clear

---

<b>Syntax</b>	<code>soft-limit-clear <i>bandwidth</i>;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture capture-group <i>client-name</i> content-destination <i>identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify a bandwidth threshold at which the latch set by the soft-limit threshold is cleared.
<b>Options</b>	<b><i>bandwidth</i></b> —Soft-limit clear threshold, in bits per second.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Content Destination on page 1330</a></li><li>• <a href="#">soft-limit on page 1365</a></li></ul>

## source-addresses

---

<b>Syntax</b>	source-addresses [ <i>addresses</i> ];
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> <a href="#">control-source</a> <i>identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	List of IP addresses from which the control source can send control protocol requests to the Juniper Networks router.
<b>Options</b>	<b><i>address</i></b> —Allowed IP source address.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Control Source on page 1331</a></li></ul>

## traceoptions (Dynamic Flow Capture)

---

<b>Syntax</b>	<pre>traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable   non-world-readable&gt;; }</pre>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable and define tracing options for dynamic flow capture events.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. Note that if you specify a maximum number for files, you must also specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000 files.</p> <p><b>Default:</b> 10 files.</p> <p><b>no-world-readable</b>—(Optional) Restrict access to the file.</p> <p><b>world-readable</b>—(Optional) Enable free access to the file.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Junos Capture Vision on page 1329</a></li></ul>

## tth

---

<b>Syntax</b>	<code>tth hops;</code>
<b>Hierarchy Level</b>	[edit services dynamic-flow-capture <a href="#">capture-group</a> <i>client-name</i> <a href="#">content-destination</a> <i>identifier</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.4.
<b>Description</b>	Time-to-live (TTL) value for the IP-IP header.
<b>Options</b>	<i>hops</i> —TTL value.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Content Destination on page 1330</a></li></ul>

## PART 6

# Link and Multilink Services

- [Link and Multilink Services Overview on page 1371](#)
- [Link and Multilink Services Configuration Guidelines on page 1375](#)
- [Summary of Multilink and Link Services Configuration Statements on page 1441](#)



# Link and Multilink Services Overview

This chapter discusses the following topics:

- [Link and Multilink Services Overview on page 1371](#)

## Link and Multilink Services Overview

---

Multilink-based protocols enable you to split, recombine, and sequence datagrams across multiple logical data links. The goal of a multilink operation is to coordinate multiple independent links between a fixed pair of systems, providing a virtual link with greater bandwidth than any of the members.

The Juniper Networks Junos operating system (Junos OS) supports several multilink-based protocols (such as MLPPP, FRF.15, and FRF.16) on the services PICs such as the Multilink Services PIC, the Link Services PIC, and the link services intelligent queuing (IQ) and voice services configured on the Adaptive Services (AS) and MultiServices PICs. For more information about link services IQ, see [“Layer 2 Service Package Capabilities and Interfaces” on page 616](#). For more information about voice services, see [“Configuring Services Interfaces for Voice Services” on page 696](#).

Starting with Junos OS Release 12.1, the following channelized MICs on MX240, MX480, and MX960 routers support Multilink Point-to-Point Protocol (MLPPP)-based services:

- 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP (MIC-3D-4CHOC3-2CHOC12)
- 8-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP (MIC-3D-8CHOC3-4CHOC12)
- 8-port Channelized DS3/E3 MIC (MIC-3D-8CHDS3-E3-B)

. For more information about Multilink Point-to-Point Protocol (MLPPP)-based services MICs, see [“Multilink Interfaces on Channelized MICs Overview” on page 1379](#).



**NOTE:** The ml- interface type is used to configure interfaces on the Multilink Services PIC and does not support class-of-service (CoS) features. The ls- interface type is used for limited CoS configurations on the Link Services PIC (except on J Series Services Routers), and the lsq- interface type is used for full CoS configurations on the Adaptive Services and MultiServices PICs. The bundle interfaces are configured on the Multiservices DPC as link services IQ (lsq) interfaces and virtual LSQ redundancy (rlsq) interfaces.

For link services IQ (lsq) interfaces, Junos OS CoS components are fully supported and are handled normally on M Series and T Series routers, as described in the *Junos OS Class of Service Library for Routing Devices*. There are some restrictions on J Series Services Routers; for more information on link services IQ configuration, see [“Layer 2 Service Package Capabilities and Interfaces” on page 616](#).

---

The Link Services and Multilink Services PICs support the following encapsulation types:

- Multilink Point-to-Point Protocol (MLPPP)
- Multilink Frame Relay (MLFR)

Starting with Junos OS Release 12.1, support for the following encapsulation types and protocols has been extended to the MX240, MX480, and MX960 routers with Multiservices DPCs:

- Multilink Point-to-Point Protocol (MLPPP)
- Multiclass MLPPP
- Multilink Frame Relay (MLFR) end-to-end (FRF.15)
- Multilink Frame Relay (MLFR) UNI NNI (FRF.16) (also referred to as MFR)
- Compressed Real-Time Transport Protocol (CRTP)

MLPPP enables you to bundle multiple PPP links into a single logical link. MLFR enables you to bundle multiple Frame Relay data-link connection identifiers (DLCIs) into a single logical link. MLPPP and MLFR provide service option granularity between low-speed T1 and E1 services and higher-speed T3 and E3 services. You use MLPPP and MLFR to increase bandwidth in smaller, more cost-effective increments. In addition to providing incremental bandwidth, bundling multiple links can add a level of fault tolerance to your dedicated access service, because you can implement bundling across multiple PICs, protecting against the failure of any single PIC.



**NOTE:** Even if the PIC can support up to 4xDS3 total throughput, each aggregate can only run a volume of traffic equal to one DS3 in bandwidth. Aggregating DS3 links is not supported.

---

At the logical unit level, the Multilink Services and Link Services PICs support the MLPPP and MLFR Frame Relay Forum (FRF) 15 encapsulation types. At the physical interface level, the Link Services PIC also supports the MLFR FRF.16 encapsulation type.

MLPPP and MLFR FRF.15 are supported on interface types **ml-fpc/pic/port**, **ls-fpc/pic/port**, and **lsq-fpc/pic/port**. For MLFR FRF.15, multiple permanent virtual circuits (PVCs) are combined into one aggregated virtual circuit (AVC). This provides fragmentation over multiple PVCs on one end and reassembly of the AVC on the other end.

MLFR FRF.16 is supported on a channelized interface, **ls-fpc/pic/port:channel**, which denotes a single MLFR FRF.16 bundle. For MLFR FRF.16, multiple links are combined to form one logical link. Packet fragmentation and reassembly occur on a per-VC basis. Each bundle can support multiple VCs. Link Services PICs can support up to 256 DLCIs per MLFR FRF.16 bundle. The physical connections must be E1, T1, channelized DS3-to-DS1, channelized DS3-to-DS0, channelized E1, channelized STM1, or channelized IQ interfaces. When you bundle channelized interfaces using the link services interface, the channelized interfaces require M Series Enhanced Flexible PIC Concentrators (FPCs).



**NOTE:** When running MLPPP or MLFR on a non-QPP interface, you cannot mix logical units that are members of an aggregate with logical units configured using other families, such as **inet**. For example, the following configuration is not valid:

```
interface e3-0/0/0 {
  encapsulation frame-relay;
  unit 99 {
    dlci 99;
    family mlfr-end-to-end {
      bundle ls-0/0/0.1;
    }
  }
  unit 100 { ## mixes mlfr with family inet
    dlci 100;
    family inet {
      address 192.168.164.53/30;
    }
  }
}
```

The standards for MLPPP, MLFR FRF.15, and MLFR FRF.16 are defined in the following specifications:

- RFC 1990, *The PPP Multilink Protocol (MP)*
- FRF.15, *End-to-End Multilink Frame Relay Implementation Agreement*
- FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*



.....

**NOTE:** Endpoint Discriminator Class compatibility checking is enabled on MLPPP interfaces. Prior to Junos OS Release 8.0, when a Juniper Networks router received an unsupported Endpoint Discriminator Class message from an MLPPP session peer, it returned an ACK response.

.....

**Related  
Documentation**

- [Understanding MLPPP Bundles and Link Fragmentation and Interleaving \(LFI\) on Serial Links on page 1381](#)
- [Example: Configuring an MLPPP Bundle on page 1420](#)
- [Example: Configuring Multilink Frame Relay FRF.15 on page 1424](#)
- [Example: Configuring Multilink Frame Relay FRF.16 on page 1427](#)

# Link and Multilink Services Configuration Guidelines

To configure multilink and link services logical interfaces, include the following statements.

```
(ml-fpc/pic/port | ls-fpc/pic/port) {
  unit logical-unit-number {
    dlcid dlcid-identifier;
    drop-timeout milliseconds;
    encapsulation type;
    fragment-threshold bytes;
    interleave-fragments;
    minimum-links number;
    mrru bytes;
    multicast-dlcid dlcid-identifier;
    short-sequence;
    family family {
      address address {
        destination address;
      }
      bundle (ml-fpc/pic/port | ls-fpc/pic/port);
    }
  }
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces]
- [edit logical-systems *logical-system-name* interfaces]

To configure link services physical interfaces, include the **mlfr-uni-nni-bundle-options** statement at the [edit interfaces *ls-fpc/pic/port:channel*] hierarchy level:

```
[edit interfaces ls-fpc/pic/port:channel]
encapsulation type;
mlfr-uni-nni-bundle-options {
  acknowledge-retries number;
  acknowledge-timer milliseconds;
  action-red-differential-delay (disable-tx | remove-link);
  drop-timeout milliseconds;
  fragment-threshold bytes;
  hello-timer milliseconds;
```

```
lmi-type (ansi | itu);
minimum-links number;
mrru bytes;
n391 number;
n392 number;
n393 number;
red-differential-delay milliseconds;
t391 number;
t392 number;
yellow-differential-delay milliseconds;
}
```

This chapter contains the following sections:

- [Multilink and Link Services PICs Overview on page 1377](#)
- [Multilink Interfaces on Channelized MICs Overview on page 1379](#)
- [Understanding MLPPP Bundles and Link Fragmentation and Interleaving \(LFI\) on Serial Links on page 1381](#)
- [Configuring the Number of Bundles on Link Services PICs on page 1383](#)
- [Configuring the Links in a Multilink or Link Services Bundle on page 1383](#)
- [Multilink and Link Services Logical Interface Configuration Overview on page 1385](#)
- [Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386](#)
- [Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces on page 1387](#)
- [Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389](#)
- [Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces on page 1390](#)
- [Configuring MRRU on Multilink and Link Services Logical Interfaces on page 1391](#)
- [Configuring the Sequence Header Format on Multilink and Link Services Logical Interfaces on page 1392](#)
- [Configuring DLCIs on Link Services Logical Interfaces on page 1393](#)
- [Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces on page 1394](#)
- [Configuring Link Services Physical Interfaces on page 1397](#)
- [Configuring CoS on Link Services Interfaces on page 1401](#)
- [Examples: Configuring Multilink Interfaces on page 1406](#)
- [Examples: Configuring Link Interfaces on page 1410](#)
- [Example: Configuring an MLPPP Bundle on page 1420](#)
- [Example: Configuring Multilink Frame Relay FRF.15 on page 1424](#)
- [Example: Configuring Multilink Frame Relay FRF.16 on page 1427](#)
- [Example: Configuring Link Interfaces on Channelized MICs on page 1430](#)

## Multilink and Link Services PICs Overview

Each Multilink Services or Link Services PIC can support a number of *bundles*. A bundle can contain up to eight individual *links*.

For Multilink Services PICs, the links can be T1, E1, or DS0 physical interfaces, and each link is associated with a logical unit number that you configure. For Link Services PICs, the links can be E1, T1, channelized DS3-to-DS1, channelized DS3-to-DS0, channelized E1, channelized STM1 interfaces, or channelized IQ interfaces. For MLFR FRF.16 bundles, each link is associated with a channel number that you configure.

You must configure a link before it can join a bundle. Each bundle should consist solely of one type of link; the mixing of physical interfaces of differing speeds within a bundle is not supported.



**NOTE:** On both Juniper Networks J Series Services Routers and M Series Multiservice Edge Routers, only one DS3 link is allowed in an MLFR bundle. MLPPP bundles can include two DS3 links.

Three versions of Multilink Services and three versions of Link Services PICs are available, as shown in [Table 38 on page 1377](#). The PIC hardware is identical, except for different faceplates that enable you to identify which version you are installing. The software limits the unit numbers and maximum number of physical interfaces you assign to the PIC.

**Table 38: Multilink and Link Services PIC Capacities**

PIC Capacity	Unit Numbers	Maximum Number of T1/DS0 Interfaces	Maximum Number of E1 Interfaces
4-bundle PIC	0 through 3	32 links	32 links
32-bundle PIC	0 through 31	256 links	219 links
128-bundle PIC	0 through 127	292 links	219 links

A single PIC can support an aggregate bandwidth of 450 megabits per second (Mbps).

You can configure a larger number of links, but the Multilink Services and Link Services PICs can reliably process only 450 Mbps of traffic. A higher rate of traffic might degrade performance.



**NOTE:** In Junos OS releases 9.0 and above you are not allowed to configure a unit number greater than the maximum unit number available on your link services PIC. Attempting to do so will cause an error message.

### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)

- [Multilink Interfaces on Channelized MICs Overview on page 1379](#)
- [Multilink and Link Services Logical Interface Configuration Overview on page 1385](#)
- [Understanding MLPPP Bundles and Link Fragmentation and Interleaving \(LFI\) on Serial Links on page 1381](#)
- [Configuring the Number of Bundles on Link Services PICs on page 1383](#)
- [Configuring the Links in a Multilink or Link Services Bundle on page 1383](#)

## Multilink Interfaces on Channelized MICs Overview

---

Multiservices Modular Interface Cards (MICs) enable you to perform multiple services on the same MIC by configuring a set of services and applications such as voice services and Layer 2 Tunneling Protocol (L2TP) services. On Juniper Networks MX Series 3D Universal Edge Routers, the Multiservices DPC provides essentially the same capabilities as the Multiservices PIC. The interfaces on both platforms are configured in the same way. The Multilink interfaces are hosted on a channelized MIC. The bundle interfaces are configured on Multiservices DPC as virtual LSQ redundancy (rlsq) interfaces.

Starting with Junos OS Release 12.1, the following channelized MICs on MX240, MX480, and MX960 routers support Multilink Point-to-Point Protocol (MLPPP)-based services:

- 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP (MIC-3D-4CHOC3-2CHOC12)
- 8-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP (MIC-3D-8CHOC3-4CHOC12)
- 8-port Channelized DS3/E3 MIC (MIC-3D-8CHDS3-E3-B)

The following encapsulations, interfaces, protocol, and packet types are supported on the aforementioned MICs:

- Multilink Point-to-Point Protocol (MLPPP)—Supports Priority-based Flow Control (PFC) for data packets and Link Control Protocol (LCP) for control packets. Compressed Real-Time Transport Protocol (CRTP) and Multiclass MLPPP are supported for both data and control packets.
- Multilink Frame Relay (MLFR) end-to-end (FRF.15)—Supports Ethernet Local Management Interface (LMI), Consortium LMI (C-LMI), and Link Integrity Protocol (LIP) for data and control packets.
- Multilink Frame Relay (MFR) UNI NNI (FRF.16)—Supports Ethernet Local Management Interface (LMI), Consortium LMI (C-LMI), and Link Integrity Protocol (LIP) for data and control packets.
- Link fragmentation and interleaving (LFI) non multilink MLPPP and MLFR packets.

Layer 2 services and voice services functionality are implemented on the Multiservices Dense Port Concentrators which supports the following two kinds of traffic that are routed by the Packet Forwarding Engine:

- Customer-end to provider-end (also, known as customer traffic)—Here, the Multilink fragments from the customer end arrive at the Multiservices interfaces configured on the channelized MIC. These fragments are then transmitted to the Multiservices DPC for Layer 2 processing such as CoS and are reassembled by the Multiservices software running on the Multiservices DPC. These reassembled packets are sent to the Packet Forwarding Engine where they go through the regular router lookup process and are finally sent over the Internet to the provider end. The voice packets also go through the same process.
- Provider-end to customer-end (also, known as Internet traffic)—Here, the data packets that are sent from the Internet provider end are received at any generic ingress interface in the Packet Forwarding Engine. These packets are then sent to the Multiservices DPC for Layer 2 processing. The Multiservices software running on Multiservices DPC

fragment these data packets and send it to the Packet Forwarding Engine. These Multilink fragments are sent over the channelized MIC interfaces to the customer end. The voice packets also go through the same process.



**NOTE:** All the features that are supported on Multilink and Link Services PICs are also supported on the Multilink Services or Link Services MICs. For more information about Multilink and Link Services PICs, see [“Multilink and Link Services PICs Overview” on page 1377](#).

Support for the following encapsulations, interfaces, protocol, and packet types are now extended to the aforementioned MICs:

- Multilink Point-to-Point Protocol (MLPPP)—Supports priority-based flow control (PFC) for data packets and Link Control Protocol (LCP) for control packets. Compressed Real-Time Transport Protocol (CRTP) and multiclass MLPPP are supported for both data and control packets.
- Multilink Frame Relay (MLFR) end-to-end (FRF.15)—Supports Ethernet Local Management Interface (LMI) and Consortium LMI (C-LMI) for data and control packets.
- Multilink Frame Relay (MLFR) UNI NNI (FRF.16)—Supports Ethernet Local Management Interface (LMI), Consortium LMI (C-LMI), and Link Integrity Protocol (LIP) for data and control packets.
- Link fragmentation and interleaving (LFI) on multilink MLPPP and MLFR packets—Reduces delay and jitter on links by breaking up large data packets and interleaving delay-sensitive voice packets with the resulting smaller packets.

#### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)
- [Example: Configuring Link Interfaces on Channelized MICs on page 1430](#)
- [Example: Configuring an MLPPP Bundle on page 1420](#)
- [Example: Configuring Multilink Frame Relay FRF.15 on page 1424](#)
- [Example: Configuring Multilink Frame Relay FRF.16 on page 1427](#)

## Understanding MLPPP Bundles and Link Fragmentation and Interleaving (LFI) on Serial Links

MX240, MX480, and MX960 3D Universal Edge Routers support MLPPP and MLFR multilink encapsulations. MLPPP enables you to bundle multiple PPP links into a single multilink bundle, and MLFR enables you to bundle multiple Frame Relay data-link connection identifiers (DLCIs) into a single multilink bundle. Multilink bundles provide additional bandwidth, load balancing, and redundancy by aggregating low-speed links, such as T1, E1, and serial links.

You configure multilink bundles as logical units or channels on the link services interface `lsq-0/0/0`:

- With MLPPP and MLFR FRF.15, multilink bundles are configured as logical units on **lsq-0/0/0**—for example, **lsq-0/0/0.0** and **lsq-0/0/0.1**.
- With MLFR FRF.16, multilink bundles are configured as channels on **lsq-0/0/0**—for example, **lsq-0/0/0:0** and **lsq-0/0/0:1**.

After creating multilink bundles, you add constituent links to the bundle. The constituent links are the low-speed physical links that are to be aggregated. You can create 64 multilink bundles, and on each multilink bundle you can add up to 8 constituent links. The following rules apply when you add constituent links to a multilink bundle:

- On each multilink bundle, add only interfaces of the same type. For example, you can add either T1 or E1, but not both.
- Only interfaces with a PPP encapsulation can be added to an MLPPP bundle, and only interfaces with a Frame Relay encapsulation can be added to an MLFR bundle.
- If an interface is a member of an existing bundle and you add it to a new bundle, the interface is automatically deleted from the existing bundle and added to the new bundle.

Configuring a multilink bundle on the two serial links increases the bandwidth by 70 percent from approximately 1 Mbps to 1.7 Mbps and prepends each packet with a multilink header as specified in the FRF.12 standard. To increase the bandwidth further, you can add up to eight serial links to the bundle. In addition to a higher bandwidth, configuring the multilink bundle provides load balancing and redundancy. If one of the serial links fails, traffic continues to be transmitted on the other links without any interruption. In contrast, independent links require routing policies for load balancing and redundancy. Independent links also require IP addresses for each link as opposed to one IP address for the bundle. In the routing table, the multilink bundle is represented as a single interface.

Starting with Junos OS Release 13.3, if you attempt to delete or deactivate a static inline service (**si**) MLPPP bundle interface that is still referenced by a member link interface, which could be PPPoE (**pp0**) or **si** logical interfaces, and commit the configuration, the commit operation fails. You must reactivate such MLPPP bundle interface before committing the settings. Alternatively, you must ensure that member links do not refer a static MLPPP bundle before you delete or deactivate the bundle. This method of deactivation and reactivation of an MLPPP bundle is not applicable for interfaces other than **si**- interfaces, such as link services IQ (**lsq-**) and virtual LSQ redundancy (**rlsq-**) interfaces.

#### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)
- [Multilink Interfaces on Channelized MICs Overview on page 1379](#)
- [Example: Configuring Link Interfaces on Channelized MICs on page 1430](#)
- [Example: Configuring an MLPPP Bundle on page 1420](#)
- [Example: Configuring Multilink Frame Relay FRF.15 on page 1424](#)
- [Example: Configuring Multilink Frame Relay FRF.16 on page 1427](#)

## Configuring the Number of Bundles on Link Services PICs

You can combine MLFR FRF.16, MLPPP, and MLFR FRF.15 bundles on a single Link Services PIC. For a sample configuration, see [“Example: Configuring a Link Services Interface with Two Links” on page 1411](#).

To configure the number of bundles on a Link Services PIC, include the **mlfr-uni-nni-bundles** statement at the **[edit chassis fpc slot-number pic pic-number]** hierarchy level:

```
mlfr-uni-nni-bundles number;
```

Each Link Services PIC can accommodate a maximum of 256 MLFR UNI NNI bundles. For more information, see the *Junos OS Administration Library for Routing Devices*.

A link can associate with one link services bundle only. All Link Services PICs support up to 256 single-link bundles and up to 256 DLCIs. For an example configuration, see the configuration examples.



**NOTE:** When one or more links in a bundle are put in loopback, reassembly buffering and hence processing are reduced so as to not affect other bundles. This prevents packet loss on other bundles, while reducing the reassembly buffers available for the bundle with looped links.

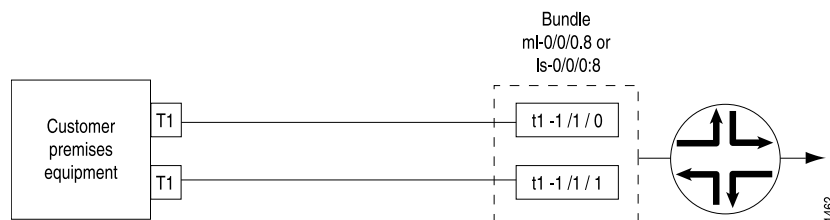
### Related Documentation

- [Example: Configuring a Link Services Interface with Two Links on page 1411](#)
- [Example: Configuring a Link Services Interface with MLPPP on page 1412](#)
- [Example: Configuring a Link Services Interface with MLFR FRF.15 on page 1413](#)
- [Example: Configuring a Link Services PIC with MLFR FRF.16 on page 1413](#)
- [Example: Configuring Link and Voice Services Interfaces with a Combination of Bundle Types on page 1414](#)

## Configuring the Links in a Multilink or Link Services Bundle

To complete a multilink or link services interface configuration, you need to configure both the physical interface and the multilink or link services bundle. For multilink interfaces, you configure the link bundle on the logical unit. For link services interfaces, you configure the link bundle as a channel (see [Figure 26 on page 1384](#)). The physical interface is usually connected to networks capable of supporting MLPPP or MLFR (FRF.15 or FRF.16).

Figure 26: Multilink Interface Configuration



The following sample configuration refers to the topology in [Figure 26 on page 1384](#) and configures a multilink or link services bundle over a T1 connection (for which the T1 physical interface is already configured).

1. To configure a physical T1 link for MLPPP, include the following statements at the `[edit interfaces t1-fpc/pic/port]` hierarchy level:

```
unit 0 {
  family mlppp {
    bundle (ml-fpc/pic/port | ls-fpc/pic/port);
  }
}
```

You do not need to configure an IP address on this link.

To configure a physical T1 link for MLFR FRF.16, include the following statements at the `[edit interfaces t1-fpc/pic/port]` hierarchy level:

```
encapsulation multilink-frame-relay-uni-nni;
unit 0 {
  family mlfr-uni-nni {
    bundle ls-fpc/pic/port:channel;
  }
}
```

You do not need to configure an IP address or a DLCI on this link.

2. To configure the logical address for the MLPPP, MLFR FRF.15, or MLFR FRF.16 bundle, include the **address** and **destination** statements:

```
address address {
  destination address;
}
```

You can include these statements at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family inet]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet]`

When you add statements such as **mrru** to the configuration and commit, the T1 interface becomes part of the multilink bundle.



**NOTE:** For MLPPP and MLFR (FRF.15 and FRF.16) links, you must specify the subnet address as /32 or /30. Any other subnet designation is treated as a mismatch.

#### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)
- [Configuring the Number of Bundles on Link Services PICs on page 1383](#)
- [Example: Configuring an MLPPP Bundle on page 1420](#)

## Multilink and Link Services Logical Interface Configuration Overview

You configure multilink and link services interface properties at the logical unit level. Default settings for multilink and link services logical interface properties are described in “[Default Settings for Multilink and Link Services Logical Interfaces](#)” on page 1385.

For general information about logical unit properties or **family inet** properties, see the *Junos OS Network Interfaces Library for Routing Devices*. For information about multilink and link services properties you configure at the **family inet** hierarchy level, see “[Configuring the Links in a Multilink or Link Services Bundle](#)” on page 1383.



**NOTE:** On DS0, E1, or T1 interfaces in LSQ bundles, you can configure the **bandwidth** statement, but the router does not use the bandwidth value if the interfaces are included in an MLPPP or MLFR bundle. The bandwidth is calculated internally according to the time slots, framing, and byte-encoding of the interface. For more information about logical interface properties, see the *Junos OS Network Interfaces Library for Routing Devices*.

## Default Settings for Multilink and Link Services Logical Interfaces

[Table 39 on page 1385](#) lists the default settings for multilink and link services statements, together with the other permitted values or value ranges.

**Table 39: Multilink and Link Services Logical Interface Statements**

Option	Default Value	Possible Values
DLCI	None	16 through 1022
Drop timeout period	500 ms for bundles greater than or equal to the T1 bandwidth value and 1500 ms for other bundles.	0 through 2000 milliseconds
Encapsulation	For multilink interfaces, <b>multilink-ppp</b> . For link services interfaces, <b>multilink-frame-relay-end-to-end</b> .	<b>multilink-frame-relay-end-to-end</b> , <b>multilink-ppp</b>

**Table 39: Multilink and Link Services Logical Interface Statements (*continued*)**

Option	Default Value	Possible Values
Fragmentation threshold	0 bytes	128 through 16,320 bytes (N×64)
Interleave fragments	disabled	enabled, disabled
Minimum links	1 link	1 through 8 links
Maximum received reconstructed unit (MRRU)	1504 bytes	1500 through 4500 bytes
Sequence ID format for MLPPP	24 bits	12 or 24 bits
Sequence ID format for MLFR FRF.15 and FRF.16	12 bits	12 bits

See “[Default Settings for Link Services Interfaces](#)” on [page 1397](#) for statements that apply to link services physical interfaces only.

#### Related Documentation

- [Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386](#)
- [Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces on page 1387](#)
- [Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389](#)
- [Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces on page 1390](#)
- [Configuring MRRU on Multilink and Link Services Logical Interfaces on page 1391](#)
- [Configuring the Sequence Header Format on Multilink and Link Services Logical Interfaces on page 1392](#)
- [Configuring DLCIs on Link Services Logical Interfaces on page 1393](#)
- [Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces on page 1394](#)

## Configuring Encapsulation for Multilink and Link Services Logical Interfaces

Multilink and link services interfaces support the following logical interface encapsulation types:

- MLPPP
- MLFR end-to-end

By default, the logical interface encapsulation type on multilink interfaces is MLPPP. The default logical interface encapsulation type on link services interfaces is MLFR end-to-end. For general information on encapsulation, see the *Junos OS Network Interfaces Library for Routing Devices*.

You can also configure physical interface encapsulation on link services interfaces. For more information, see “[Configuring Encapsulation for Link Services Physical Interfaces](#)” on page 1398.

To configure multilink or link services encapsulation, include the **encapsulation** statement:

**encapsulation** *type*;

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

You must also configure the T1, E1, or DS0 physical interface with the same encapsulation type.



**CAUTION:** When you configure the first MLFR encapsulated unit or delete the last MLFR encapsulated unit on a port, it triggers an interface encapsulation change on the port, which causes an interface flap on the other units within the port that are configured with generic Frame Relay.

#### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)
- [Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces on page 1387](#)
- [Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389](#)
- [Example: Configuring a Link Services Interface with MLPPP on page 1412](#)
- [encapsulation \(Logical Interface\) on page 1448](#)

## Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces

By default, the drop timeout parameter is disabled. You can configure a drop timeout value to provide a recovery mechanism if individual links in the multilink or link services bundle drop one or more packets. Drop timeout is not a differential delay tolerance setting, and does not limit the overall latency. However, you need to make sure the value you set is larger than the expected differential delay across the links, so that the timeout period does not elapse under normal jitter conditions, but only when there is actual packet loss. You can configure differential delay tolerance for link services interfaces only. For more information, see “[Configuring Differential Delay Alarms on Link Services Physical Interfaces with MLFR FRF.16](#)” on page 1399.

To configure the drop timeout value, include the **drop-timeout** statement:

```
drop-timeout milliseconds;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

For link services interfaces, you also can configure the drop timeout value at the physical interface level by including the **drop-timeout** statement at the [edit interfaces *ls-fpc/pic/port:channel* mlfr-uni-nni-bundle-options] hierarchy level:

```
drop-timeout milliseconds;
```

By default, the drop timer has a value of 500 ms for bundles greater than or equal to the T1 bandwidth value, and 1500 ms for other bundles. Any CLI-configured value overrides these defaults. Values can range from 1 through 2000 milliseconds. Values less than 5 milliseconds are not recommended, and a configured value of 0 reverts to the default value of 2000 milliseconds.



**NOTE:** For multilink or link services interfaces, if a packet or fragment encounters an error condition and is destined for a disabled bundle or link, it does not contribute to the dropped packet and frame counts in the per-bundle statistics. The packet is counted under the global error statistics and is not included in the global output bytes and output packet counts. This unusual accounting happens only if the error conditions are generated inside the multilink interface, not if the packet encounters errors on the wire or elsewhere in the network.

If you configure the **drop-timeout** statement with a value of 0, it disables any resequencing by the PIC for the specified class of MLPPP traffic. Packets are forwarded with the assumption that they arrived in sequence, and forwarding of fragmented packets is disabled for all classes. Fragments dropped as a result of this setting will increment the counter at the class level.

Alternatively, you can configure the **drop-timeout** statement at the [edit class-of-service fragmentation-maps *map-name* forwarding-class *class*] hierarchy level. The behavior and the default and range values are identical, but the setting applies only to the specified forwarding class. Configuration at the bundle level overrides configuration at the class-of-service level.

By default, compression of the inner PPP header in the MLPPP payload is enabled. To disable compression, include the **disable-mlppp-inner-ppp-pfc** statement at the [edit interfaces *interface-name* unit *logical-unit-number*] hierarchy level. For example:

```
interfaces lsq-1/2/0 {
  unit 0 {
    encapsulation multilink-ppp;
    disable-mlppp-inner-ppp-pfc;
```

```

    multilink-max-classes 4;
    family inet {
        address 10.50.1.2/30;
    }
}

```

For more information about CoS configuration, see the *Junos OS Class of Service Library for Routing Devices*. You can view the configured drop-timeout value and the status of inner PPP header compression by issuing the **show interfaces *interface-name* extensive** command.

#### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)
- [Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386](#)
- [Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389](#)
- [Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces on page 1390](#)

## Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces

For multilink and link services logical interfaces with MLPPP encapsulation only, you can configure a *fragmentation threshold* to limit the size of packet payloads transmitted across the individual links within the multilink circuit. The software splits any incoming packet that exceeds the fragmentation threshold into smaller units suitable for the circuit size; it reassembles the fragments at the other end, but does not affect the output traffic stream. The threshold value affects the payload only; it does not affect the MLPPP header. By default, the fragmentation threshold parameter is disabled.



**NOTE:** To ensure proper load balancing:

- For Link Services MLFR (FRF.15 and FRF.16) interfaces, do not include the **fragment-threshold** statement in the configuration.
- For MLPPP interfaces, do not include both the **fragment-threshold** statement and the **short-sequence** statement in the configuration.
- For MLFR (FRF.15 and FRF.16) and MLPPP interfaces, if the MTU of links in a bundle is less than the bundle MTU plus encapsulation overhead, then fragmentation is automatically enabled. You should avoid this situation for MLFR (FRF.15 and FRF.16) interfaces and for MLPPP interfaces on which short-sequencing is enabled.

To configure a fragmentation threshold value, include the **fragment-threshold** statement:

**fragment-threshold** *bytes*;

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

For link services interfaces, you also can configure a fragmentation threshold value at the physical interface level by including the **fragment-threshold** statement at the **[edit interfaces *ls-fpc/pic/port:channel* mlfr-uni-nni-bundle-options]** hierarchy level:

**fragment-threshold** *bytes*;

The maximum fragment size can be from 128 through 16,320 bytes. The Junos OS automatically subdivides packet payloads that exceed this value. Any value you set must be a multiple of 64 bytes (Nx64). The default value, 0, results in no fragmentation.

#### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)
- [Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386](#)
- [Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces on page 1387](#)
- [Example: Configuring a Multilink Interface with MLPPP on page 1407](#)
- [fragment-threshold on page 1451](#)

---

## Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces

---

You can set the minimum number of links that must be up for the multilink bundle as a whole to be labeled up. By default, only one link must be up for the bundle to be labeled up. A member link is considered up when the PPP Link Control Protocol (LCP) phase transitions to open state.

The **minimum-links** value should be identical on both ends of the bundle.

To set the minimum number, include the **minimum-links** statement:

**minimum-links** *number*;

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

For link services interfaces, you also can configure the minimum number of links at the physical interface level by including the **minimum-links** statement at the **[edit interfaces *ls-fpc/pic/port:channel* mlfr-uni-nni-bundle-options]** hierarchy level:

**minimum-links** *number*;

The number can be from 1 through 8. The maximum number of links supported in a bundle is 8. When 8 is specified, all configured links of a bundle must be up.

- Related Documentation**
- [Link and Multilink Services Overview on page 1371](#)
  - [Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386](#)
  - [Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces on page 1387](#)
  - [Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389](#)
  - [Configuring MRRU on Multilink and Link Services Logical Interfaces on page 1391](#)

## Configuring MRRU on Multilink and Link Services Logical Interfaces

The *maximum received reconstructed unit (MRRU)* is similar to a maximum transmission unit (MTU), but applies only to multilink bundles; it is the maximum packet size that the multilink interface can process. By default, the MRRU is set to 1500 bytes; you can configure a different MRRU value if the peer equipment allows this. The MRRU accounts for the original payload, for example the Layer 3 protocol payload, but does not include the 2-byte PPP header or the additional MLPPP or MLFR header applied while the individual multilink packets are traversing separate links in the bundle.

To configure a different MRRU value, include the **mrru** statement:

```
mrru bytes;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

For link services interfaces, you also can configure a different MRRU at the physical interface level by including the **mrru** statement at the **[edit interfaces *ls-fpc/pic/port:channel* mlfr-uni-nni-bundle-options]** hierarchy level:

```
mrru bytes;
```

The MRRU size can range from 1500 through 4500 bytes.



**NOTE:** If you set the MRRU on a bundle to a value larger than the MTU of the individual links within it, you must enable a fragmentation threshold for that bundle. Set the threshold to a value no larger than the smallest MTU of any link included in the bundle.

Determine the appropriate MTU size for the bundle by ensuring that the MTU size does not exceed the sum of the encapsulation overhead and the MTU sizes for the links in the bundle.

You can configure separate **family mtu** values on the following protocol families under bundle interfaces: **inet**, **inet6**, **iso**, and **mpls**. If not configured, the default value of 1500 is used on all except for **mpls** configurations, in which the value 1488 is used.



**NOTE:** The effective family MTU might be different from the MTU value specified for MLPPP configurations, because it is adjusted downward by the remote MRRU's constraints. The remote MRRU configuration is not supported on M120 routers.

**Related Documentation**

- [Link and Multilink Services Overview on page 1371](#)
- [Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386](#)
- [Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces on page 1387](#)
- [Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389](#)
- [Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces on page 1390](#)

---

## Configuring the Sequence Header Format on Multilink and Link Services Logical Interfaces

---

For MLPPP, the sequence header format is set to 24 bits by default. You can configure an alternative value of 12 bits, but 24 bits is considered the more robust value for most networks.

To configure a different sequence header value, include the **short-sequence** statement:

**short-sequence;**

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

For MLFR FRF.15, the sequence header format is set to 24 bits by default. This is the only valid option.

**Related Documentation**

- [Link and Multilink Services Overview on page 1371](#)
- [Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces on page 1387](#)
- [Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389](#)

- [Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces on page 1390](#)
- [Configuring MRRU on Multilink and Link Services Logical Interfaces on page 1391](#)
- [Configuring DLCIs on Link Services Logical Interfaces on page 1393](#)

## Configuring DLCIs on Link Services Logical Interfaces

---

For link services interfaces only, you can configure multiple DLCIs for MLFR FRF.16 or MLPPP bundles.

DLCIs are not supported on multilink interfaces.

### Configuring Point-to-Point DLCIs for MLFR FRF.16 and MLPPP Bundles

For link services interfaces only, you can configure multiple point-to-point DLCIs for each MLFR FRF.16 or MLPPP bundle. A channelized interface, such as `ls-1/1/1:0`, denotes a single MLFR FRF.16 bundle. To configure a DLCI, include the `dlci` statement:

```
dlci dlci-identifier;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

The DLCI identifier is a value from 16 through 1022. Numbers 1 through 15 are reserved for future use.

When you configure point-to-point connections, the maximum transmission unit (MTU) sizes on both sides of the connection must be the same.

### Configuring Multicast-Capable DLCIs for MLFR FRF.16 Bundles

For link services interfaces only, you can configure multiple multicast-capable DLCIs for each MLFR FRF.16 bundle. A channelized interface, such as `ls-1/1/1:0`, denotes a single MLFR FRF.16 bundle. By default, Frame Relay connections assume unicast traffic. If your Frame Relay switch performs multicast replication, you can configure the link services connection to support multicast traffic by including the `multicast-dlci` statement:

```
multicast-dlci dlci-identifier;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

The DLCI identifier is a value from 16 through 1022 that defines the Frame Relay DLCI over which the switch expects to receive multicast packets for replication.

You can configure multicast support only on point-to-multipoint link services connections. Multicast-capable DLCIs are not supported on multilink interfaces.

If keepalives are enabled, causing the interface to send Local Management Interface (LMI) messages during idle times, the number of possible DLCI configurations is limited by the MTU selected for the interface. For more information, see [“Configuring Keepalives on Link Services Physical Interfaces” on page 1400](#).

**Related  
Documentation**

- [Link and Multilink Services Overview on page 1371](#)
- [Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389](#)
- [Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces on page 1390](#)
- [Configuring MRRU on Multilink and Link Services Logical Interfaces on page 1391](#)
- [Configuring the Sequence Header Format on Multilink and Link Services Logical Interfaces on page 1392](#)

---

## Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces

---

For link services FRF.15 and MLPPP interfaces only, you can configure link fragment interleaving (LFI). LFI reduces excessive delays of Frame Relay packets by fragmenting long packets into smaller packets and interleaving them with real-time frames. This allows real-time and non-real-time data frames to be carried together on lower-speed links without causing excessive delays to the real-time traffic. When the peer interface receives the smaller fragments, it reassembles the fragments into their original packet. For example, short delay-sensitive packets, such as packetized voice, can race ahead of larger delay-insensitive packets, such as common data packets.



**NOTE:** All Link Services PICs (4-multilink bundle, 32-multilink bundle, and 128-multilink bundle) support up to 256 link services interfaces with LFI enabled, if those link services interfaces contain only one constituent link each. For the Link Services PIC, multiple-link LFI bundles are simply multilink bundles, and are limited based on the type of PIC (4-multilink bundle, 32-multilink bundle, and 128-multilink bundle).

In addition, the multilink bundles you configure subtract from the total of 256 possible LFI-enabled link services interfaces. For example, if a 32-multilink bundle Link Services PIC has 24 multilink bundles configured and active, then you can configure  $256 - 24 = 232$  LFI-enabled link services interfaces, each with a single constituent link.

For link services IQ interfaces (lsq), the `interleave-fragments` statement is not valid. Instead, you can enable LFI by configuring fragmentation maps. For more information, see [“Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces” on page 633](#).

---

You can configure multiple links in a bundle and configure packet interleaving. However, if you use packet interleaving, high-priority, nonmultilink-encapsulated packets use a hash-based algorithm to choose a single link.

For detailed information about link services CoS, see [“Configuring CoS on Link Services Interfaces” on page 1401](#).

Per-bundle CoS queuing is supported on link services IQ interfaces (**lsq**). For more information about link services IQ interfaces, see [“Layer 2 Service Package Capabilities and Interfaces” on page 616](#).

The Junos OS supports end-to-end fragmentation in compliance with the FRF.12 *Frame Relay Fragmentation Implementation Agreement* standard. Unlike user-to-network interface (UNI) and network-to-network (NNI) fragmentation, end-to-end supports fragmentation only at the endpoints.

By default, packet interleaving is disabled. To enable packet interleaving, include the **interleave-fragments** statement:

```
interleave-fragments;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

## Configuring LFI with DLCI Scheduling

For Link Services and Channelized DS3 IQ PICs, you can configure LFI and DLCI scheduling. For channelized DS3 interfaces, LFI is supported with FRF.15 only, and on M10i and M20 platforms only.

Configuring LFI with DLCI scheduling enables packets entering the Link Services PIC to be fragmented before being transmitted to the Channelized DS3 IQ PIC. Once the fragmented packets enter the Channelized DS3 IQ PIC, they are scheduled at the DLCI level, to allow priority transmission for real-time applications.

For more information about associating a scheduler with a DLCI, see the *Junos OS Class of Service Library for Routing Devices*.

### Example: Configuring LFI with DLCI Scheduling

Configure packets entering the Link Services PIC to be fragmented before being transmitted to the Channelized DS3 IQ PIC. Once the fragmented packets enter the Channelized DS3 IQ PIC, they are scheduled at the DLCI level, to allow priority transmission for real-time applications.

```
[edit interfaces]
ls-1/0/0 {
  unit 1 {
    encapsulation multilink-frame-relay-end-to-end;
    interleave-fragments;
```

```
family inet {
  address 192.168.5.2/32 {
    destination 192.168.5.3;
  }
}
}
t3-1/0/0:1 {
  per-unit-scheduler;
  unit 0 {
    dlci 16;
    encapsulation multilink-frame-relay-end-to-end;
    family mlfr-end-to-end {
      bundle ls-1/0/0.1;
    }
  }
}
[edit class-of-service]
interfaces {
  t3-1/0/0:1 {
    unit 0 {
      scheduler-map sched-map-logical-0;
      shaping-rate 10m;
    }
    unit 1 {
      scheduler-map sched-map-logical-1;
      shaping-rate 20m;
    }
  }
}
scheduler-maps {
  sched-map-logical-0 {
    forwarding-class best-effort scheduler sched-best-effort-0;
    forwarding-class assured-forwarding scheduler sched-bronze-0;
    forwarding-class expedited-forwarding scheduler sched-silver-0;
    forwarding-class network-control scheduler sched-gold-0;
  }
  sched-map-logical-1 {
    forwarding-class best-effort scheduler sched-best-effort-1;
    forwarding-class assured-forwarding scheduler sched-bronze-1;
    forwarding-class expedited-forwarding scheduler sched-silver-1;
    forwarding-class network-control scheduler sched-gold-1;
  }
}
schedulers {
  sched-best-effort-0 {
    transmit-rate 4m;
  }
  sched-bronze-0 {
    transmit-rate 3m;
  }
  sched-silver-0 {
    transmit-rate 2m;
  }
  sched-gold-0 {
    transmit-rate 1m;
  }
  sched-best-effort-1 {
```

```

        transmit-rate 8m;
    }
    sched-bronze-1 {
        transmit-rate 6m;
    }
    sched-silver-1 {
        transmit-rate 4m;
    }
    sched-gold-1 {
        transmit-rate 2m;
    }
}
}

```

#### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)
- [Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces on page 1390](#)
- [Configuring MRRU on Multilink and Link Services Logical Interfaces on page 1391](#)
- [Configuring the Sequence Header Format on Multilink and Link Services Logical Interfaces on page 1392](#)
- [Configuring DLCIs on Link Services Logical Interfaces on page 1393](#)

## Configuring Link Services Physical Interfaces

You configure link services interface properties at the logical unit and physical interface level. Default settings for link services physical interface properties are described in “Default Settings for Link Services Interfaces” on page 1397.

The following sections explain how to configure link services physical interfaces:

- [Default Settings for Link Services Interfaces on page 1397](#)
- [Configuring Encapsulation for Link Services Physical Interfaces on page 1398](#)
- [Configuring Acknowledgment Timers on Link Services Physical Interfaces on page 1399](#)
- [Configuring Differential Delay Alarms on Link Services Physical Interfaces with MLFR FRF.16 on page 1399](#)
- [Configuring Keepalives on Link Services Physical Interfaces on page 1400](#)

For information about link services physical interface properties that can also be configured at the logical unit level, see “Multilink and Link Services Logical Interface Configuration Overview” on page 1385.

## Default Settings for Link Services Interfaces

[Table 40 on page 1398](#) lists the default settings for link services statements, together with the other permitted values or value ranges.

Table 40: Link Services Physical Interface Statements for MLFR FRF.16

Option	Default Value	Possible Values
Action red differential delay	<b>remove-link</b>	<b>disable-tx, remove-link</b>
Red differential delay	120 ms	1 through 2000 ms
Yellow differential delay	72 ms	1 through 2000 ms
Drop timeout period	0 ms	0 through 2000 ms
Encapsulation	<b>multilink-frame-relay-uni-nni</b>	<b>multilink-frame-relay-uni-nni</b>
Fragmentation threshold	0 bytes	128 through 16,320 bytes (Nx64)
LMI type	itu	ansi, itu
Minimum links	1 link	1 through 8 links
MRRU	1504 bytes	1500 through 4500 bytes
n391 (full status polling counter)	6	1 through 255
n392 (LMI error threshold)	3	1 through 10
n393 (LMI monitored event count)	4	1 through 10
t391 (link integrity verify polling timer)	10	5 through 30
t392 (polling verification timer)	15	5 through 30
Sequence ID format for MLFR	12 bits	12 bits

## Configuring Encapsulation for Link Services Physical Interfaces

Link services interfaces support the physical interface encapsulation MLFR UNI NNI. By default, the physical interface encapsulation on link services interfaces is MLFR UNI NNI. Multilink interfaces do not support physical interface encapsulation.

For more information, see the *Junos OS Network Interfaces Library for Routing Devices*.

You can also configure logical interface encapsulation on multilink and link services interfaces. For more information, see [“Configuring Encapsulation for Multilink and Link Services Logical Interfaces”](#) on page 1386.

To explicitly configure link services physical interface encapsulation, include the **encapsulation** statement at the **[edit interfaces ls-fpc/pic/port:channel]** hierarchy level:

```
encapsulation type;
```

You must also configure the T1, E1, or DSO physical and physical interface with the same encapsulation type.

## Configuring Acknowledgment Timers on Link Services Physical Interfaces

For link services interfaces configured with MLFR FRF.16, each link end point in a bundle initiates a request for bundle operation with its peer by transmitting an add link message. A hello message notifies the peer end point that the local end point is up. Both ends of a link generate a hello message periodically, or as configured with the hello timer. A remove link message notifies the peer that the local end management is removing the link from bundle operation. End points respond to add link, remove link, and hello messages by sending acknowledgment messages.

You can configure the maximum period to wait for an add link acknowledgment, hello acknowledgment, or remove link acknowledgment by including the **acknowledge-timer** statement at the **[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]** hierarchy level:

```
acknowledge-timer milliseconds;
```

The acknowledgment timer can be from 1 through 10 milliseconds. The default is 4 milliseconds.

For link services interfaces, you can configure the number of retransmission attempts to be made for consecutive hello or remove link messages after the expiration of the acknowledgment timer by including the **acknowledge-retries** statement at the **[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]** hierarchy level:

```
acknowledge-retries number;
```

**acknowledgment-retries** can be a value from 1 through 5. The default is 2.

You can configure the rate at which hello messages are sent by including the **hello-timer** statement at the **[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]** hierarchy level:

```
hello-timer milliseconds;
```

A hello message is transmitted after the specified period (in milliseconds) has elapsed. The hello timer can be from 1 through 180 milliseconds; the default is 10 milliseconds. When the hello timer expires, a link end point generates an add-link message.

## Configuring Differential Delay Alarms on Link Services Physical Interfaces with MLFR FRF.16

For link services interfaces configured with MLFR FRF.16, the differential delay between links in a bundle is measured and warning is given when a link has a substantially greater differential delay than other links in the same bundle. The implementing endpoint can determine if the differential delay is in an acceptable range and decide to remove the link from the bundle, or to stop transmission on the link.

You can configure the yellow differential delay for links in a bundle by including the **yellow-differential-delay** statement at the **[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]** hierarchy level:

**yellow-differential-delay** *milliseconds*;

The yellow differential delay can be from 1 through 2000 milliseconds. The default is 72 milliseconds.

You can configure the red differential delay for links in a bundle to give warning by including the **red-differential-delay** statements at the **[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]** hierarchy level:

**red-differential-delay** *milliseconds*;

The red differential delay can be from 1 through 2000 milliseconds. The default is 120 milliseconds.

You can configure the action to be taken when differential delay exceeds the red limit by including the **action-red-differential-delay** **red** statements at the **[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]** hierarchy level:

**action-red-differential-delay** (disable-tx | remove-link);

The **disable-tx** option disables transmission on the link. The **remove-link** option removes the link from the bundle. The default action is **remove-link**.

You can view these settings in the output of the **show interfaces extensive lsq-fpc/pic/port:channel** command.

## Configuring Keepalives on Link Services Physical Interfaces

You can tune the keepalive settings on the physical link-services interface. By default, the Junos OS uses ITU Q.933 Annex A LMIs for FRF.16. To instead use ITU Annex A LMIs (ANSI), include the **lmi-type ansi** statement at the **[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]** hierarchy level. LMI type ANSI is used in the following example:

**lmi-type** ansi;

To configure Frame Relay keepalive parameters on a link services interface, include the **n391**, **n392**, **n393**, **t391** and **t392** statements at the **[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]** hierarchy level:

```
[edit interfaces ls-fpc/pic/port:channel mlfr-uni-nni-bundle-options]
n391 number;
n392 number;
n393 number;
t391 number;
t392 number;
```

The statements determine the indicated keepalive settings:

- **n391**—Full status polling interval. The data terminal equipment (DTE) sends a status inquiry to the data communication equipment (DCE) at the interval specified by the **t391** statement. This statement sets the frequency at which the DTE requests full status report; for example, the value **10** means that the DTE requests full status report in every tenth inquiry. The intermediate inquiries request a keepalive response only. The range is **1** through **255**, with a default of **6**.
- **n392**—Error threshold, which is the maximum number of errors that can occur during the number of events set by the **n393** statement before the link is marked inoperative. The range is **1** through **10**, with a default of **3**.
- **n393**—Monitored event count. The range is **1** through **10**, with a default of **4**.
- **t391**—The interval at which the DTE requests a keepalive response from the DCE and updates status, depending on the error threshold value. The range is **5** through **30** seconds, with a default of **10** seconds.
- **t392**—The period during which the DCE checks for keepalive responses from the DTE and updates status, depending on the DCE error threshold value. The range is from **5** through **30** seconds, with a default of **15** seconds.



**NOTE:** For the LMI to work properly, you must configure one side of a link services bundle to be a DCE.

#### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)
- [Example: Configuring a Link Services Interface with Two Links on page 1411](#)

## Configuring CoS on Link Services Interfaces

For link services IQ (**lsq-**) interfaces, Junos class of service (CoS) is fully supported and functions as described in the *Junos OS Class of Service Library for Routing Devices*. For more information and detailed configuration examples, see “[Layer 2 Service Package Capabilities and Interfaces](#)” on page 616.

On SRX Series and J Series devices, the **lsq-** interface is an internal interface, which is not associated with a physical interface. For information about link services on SRX Series and J Series devices, see the *Junos OS Interfaces Configuration Guide for Security Devices*.

For information about CoS functions and link services on M Series or T Series routers, see the following sections:

- [CoS for Link Services Interfaces on M Series and T Series Routers on page 1402](#)
- [Example: Configuring CoS on Link Services Interfaces on page 1403](#)

## CoS for Link Services Interfaces on M Series and T Series Routers

For Link Services PIC interfaces (**ls**) on M Series and T Series routers, queue 0 is the only queue that you should configure to receive fragmented packets. Configure all other queues to be higher-priority queues.

Table 41 on page 1402 summarizes how CoS queues work on link services (**ls**) interfaces.

**Table 41: Link Services CoS Queues**

Supported Bundling Type	Queue 0	Higher-Priority Queues
Hash-based load balancing	No	Yes
MLFR FRF.15	Yes	No
MLFR FRF.16	Yes	No
MLPPP	Yes	No

For M Series and T Series routers, CoS on link services (**ls**) interfaces works as follows:

- On all platforms, the Link Services PIC currently supports up to four queues: 0, 1, 2, and 3.
- Queue 0 uses MLFR FRF.15, MLFR FRF.16, or MLPPP to bundle packets.
- Higher-priority queues (1, 2, and 3) use hash-based load balancing to bundle packets. IP and MPLS header information is included in the hash.
- MLPPP packets traversing link services interfaces using queue 0 are fragmented and distributed across the constituent links. Queue 0 packets are sent on the least utilized link, proportional to its bandwidth. The queue 0 load balancer attempts to maintain even distribution of all traffic across all constituent links. In situations with a small number of high-priority traffic flows (queues 1, 2, and 3), queue 0 traffic might be unevenly distributed.
- For the MLFR FRF.16 protocol, only queue 0 works. If you configure a bundled interface to use MLFR FRF.16 with queue 0, then you must ensure the classifier does not send any traffic to queues 1, 2, and 3 on that interface.
- To carry high-priority traffic correctly on MLFR FRF.16 interfaces, you must configure an output firewall filter that forces all traffic into queue 0 on the **ls-fpc/pic/port.channel** interface.
- MLFR FRF.15 and MLPPP interfaces support CoS through packet interleaving. The MLFR FRF.16 standard does not support packet interleaving, so all packets destined for an FRF.16 PVC interface must egress from the same queue.
- For constituent link interfaces of Link Services PICs, you can configure standard scheduler maps.
- For input packets and fragments received from constituent links, you can use regular input firewall filters and standard CoS classifiers on the link services interface.

- For packets that pass through a link services interface and are destined for a constituent link interface, all traffic using queue 0 is fragmented. Traffic using higher-priority queues (1, 2, and 3) is not fragmented.
- For MLFR FRF.15 and MLPPP, routing protocol packets smaller than 128 bytes are sent to queue 3; routing protocol packets that exceed 128 bytes are sent to queue 0 and fragmented accordingly. For MLFR FRF.16, queue 0 is used for all packet sizes.
- You must configure output firewall classification for egress traffic on the link services interface, not directly on the constituent link interface directly.
- Inverse multiplexing for ATM (IMA) is not supported on link services interfaces.

For more information, see [“Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces”](#) on page 1394 and the *Routing Policy Feature Guide for Routing Devices*.

### Example: Configuring CoS on Link Services Interfaces

Configure CoS on a link services interface and its constituent link interfaces.



**NOTE:** This example applies to M Series and T Series routers. For examples that apply to SRX Series and J Series devices, see the *Junos OS Interfaces Configuration Guide for Security Devices*.

Packets that do not match the firewall filters are sent to a queue that performs load balancing by sending fragments to all constituent links.

Packets that match the firewall filters are sent to a queue that does not support packet fragmentation and reassembly; instead, this traffic is load-balanced by sending each packet flow to a different constituent link. Each packet that matches a firewall filter is subjected to a hash on the IP source address and the IP destination address to determine the packet flow to which each packet belongs.

When you configure the MLPPP encapsulation type or the multilink FRF.15 Frame Relay end-to-end encapsulation type, routing protocol packets smaller than 128 bytes are sent to the network-control queue on the constituent link interface. This keeps routing protocols operating normally, even when low-speed links are congested by regular packets.

```
[edit interfaces]
ls-7/0/0 {
  unit 0 {
    encapsulation multilink-ppp;
    interleave-fragments;
    family inet {
      filter {
        output lfi_ls_filter;
      }
      address 10.54.0.2/32 {
        destination 10.54.0.1;
      }
    }
  }
}
```

```
    }
  }
  ge-7/2/0 {
    unit 0 {
      family inet {
        address 192.168.1.1/24;
      }
    }
  }
  cel-7/3/6 {
    no-partition interface-type e1;
  }
  e1-7/3/6 {
    encapsulation ppp;
    unit 0 {
      family mlppp {
        bundle ls-7/0/0.0;
      }
    }
  }
  cel-7/3/7 {
    no-partition interface-type e1;
  }
  e1-7/3/7 {
    encapsulation ppp;
    unit 0 {
      family mlppp {
        bundle ls-7/0/0.0;
      }
    }
  }
}
[edit class-of-service]
classifiers {
  dscp dscp_default {
    import default;
  }
  inet-precedence inet-precedence_default {
    import default;
  }
}
code-point-aliases {
  dscp {
    af11 001010;
    af12 001100;
    af13 001110;
    af21 010010;
    af22 010100;
    af23 010110;
    af31 011010;
    af32 011100;
    af33 011110;
    af41 100010;
    af42 100100;
    af43 100110;
    be 000000;
    cs1 001000;
```

```

        cs2 010000;
        cs3 011000;
        cs4 100000;
        cs5 101000;
        cs6 110000;
        cs7 111000;
        ef 101110;
    }
    inet-precedence {
        af11 001;
        af21 010;
        af31 011;
        af41 100;
        be 000;
        cs6 110;
        cs7 111;
        ef 101;
        nc1 110;
        nc2 111;
    }
}
forwarding-classes {
    queue 0 be;
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
}
interfaces {
    ge-7/2/0 {
        scheduler-map sched-map;
        unit 0 {
            classifiers {
                dscp dscp_default;
            }
        }
    }
    e1-7/3/6 {
        scheduler-map sched-map;
    }
    e1-7/3/7 {
        scheduler-map sched-map;
    }
    ls-7/0/0 {
        scheduler-map sched-map;
        unit 0 {
            classifiers {
                inet-precedence inet-precedence_default;
            }
        }
    }
}
scheduler-maps {
    sched-map {
        forwarding-class af scheduler af-scheduler;
        forwarding-class be scheduler be-scheduler;
        forwarding-class ef scheduler ef-scheduler;
    }
}

```

```
        forwarding-class nc scheduler nc-scheduler;
    }
}
schedulers {
  af-scheduler {
    transmit-rate percent 25;
    buffer-size percent 25;
  }
  be-scheduler {
    transmit-rate percent 25;
    buffer-size percent 25;
  }
  ef-scheduler {
    transmit-rate percent 25;
    buffer-size percent 25;
  }
  nc-scheduler {
    transmit-rate percent 25;
    buffer-size percent 25;
  }
}
[edit firewall]
filter lfi_ls_filter {
  term term0 {
    from {
      destination-address {
        192.168.1.3/32;
      }
      precedence 5;
    }
    then {
      count count-192-168-1-3;
      forwarding-class af;
      accept;
    }
  }
  term default {
    then {
      log;
      forwarding-class best effort;
      accept;
    }
  }
}
```

**Related  
Documentation**

- [Link and Multilink Services Overview on page 1371](#)
- [Configuring Link Services Physical Interfaces on page 1397](#)

---

## Examples: Configuring Multilink Interfaces

The examples in this section include only the configuration of multilink interfaces. For information about configuring the constituent interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

The examples in this section show the following configurations:

- [Example: Configuring a Multilink Interface with MLPPP on page 1407](#)
- [Example: Configuring a Multilink Interface with MLPPP over ATM 2 Interfaces on page 1408](#)
- [Example: Configuring a Multilink Interface with MLFR FRF.15 on page 1409](#)

### Example: Configuring a Multilink Interface with MLPPP

```
[edit interfaces]
ml-1/0/0 {
  unit 1 {
    fragment-threshold 128;
    family inet {
      address 192.168.5.1/32 {
        destination 192.168.200.200;
      }
    }
  }
  unit 10 {
    family inet {
      address 10.1.1.3/32 {
        destination 10.1.1.2;
      }
    }
  }
}
t1-5/1/0 {
  unit 0 {
    family mlppp {
      bundle ml-1/0/0.1;
    }
  }
}
t1-5/1/1 {
  unit 0 {
    family mlppp {
      bundle ml-1/0/0.1;
    }
  }
}
t1-5/1/2 {
  unit 0 {
    family mlppp {
      bundle ml-1/0/0.1;
    }
  }
}
```

#### Related Documentation

- [Link and Multilink Services Overview on page 1371](#)
- [Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389](#)
- [fragment-threshold on page 1451](#)

### Example: Configuring a Multilink Interface with MLPPP over ATM 2 Interfaces

```
[edit interfaces]
at-0/0/0 {
  atm-options {
    pic-type atm2;
    vpi 10;
  }
  unit 0 {
    encapsulation atm-mlppp-llc;
    ppp-options {
      chap {
        access-profile pe-B-ppp-clients;
        local-name "pe-A-at-0/0/0";
      }
    }
    keepalive interval 5 up-count 6 down-count 4;
    vci 10.120;
    family mlppp {
      bundle ls-0/3/0.0;
    }
  }
}
at-0/0/1 {
  atm-options {
    pic-type atm2;
    vpi 11;
  }
  unit 1 {
    encapsulation atm-mlppp-llc;
    ppp-options {
      chap {
        access-profile pe-B-ppp-clients;
        local-name "pe-A-at-0/0/0";
      }
    }
    keepalive interval 5 up-count 6 down-count 4;
    vci 11.120;
    family mlppp {
      bundle ls-0/3/0.0;
    }
  }
}
at-1/2/3 {
  atm-options {
    pic-type atm2;
    vpi 12;
  }
  unit 2 {
    encapsulation atm-mlppp-llc;
    ppp-options {
      chap {
        access-profile pe-B-ppp-clients;
        local-name "pe-A-at-0/0/0";
      }
    }
  }
}
```

```

    }
    keepalive interval 5 up-count 6 down-count 4;
    vci 12.120;
    family mlppp {
        bundle ls-0/3/0.0;
    }
}
...
ls-0/3/0 {
    encapsulation multilink-ppp;
    interleave-fragments;
    keepalive;
    unit 0 {
        mrru 4500;
        short-sequence;
        fragment-threshold 16320;
        drop-timeout 2000;
        encapsulation multilink-ppp;
        interleave-fragments;
        minimum-links 8;
        family inet {
            address 10.10.0.1/32 {
                destination 10.10.0.2;
            }
        }
        family iso;
        family inet6 {
            address 2001:DB8:0:1/32 {
                destination 2001:DB8:0:2;
            }
        }
    }
}
...
}

```

- Related Documentation**
- [Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386](#)
  - [Example: Configuring a Multilink Interface with MLPPP over ATM 2 Interfaces on page 1408](#)
  - [encapsulation \(Logical Interface\) on page 1448](#)

### Example: Configuring a Multilink Interface with MLFR FRF.15

```

[edit interfaces]
ml-1/0/0 {
    unit 1 {
        encapsulation multilink-frame-relay-end-to-end;
        family inet {
            address 192.168.5.2/32 {
                destination 192.168.5.3;
            }
        }
    }
    unit 10 {
        encapsulation multilink-frame-relay-end-to-end;
    }
}

```

```
family inet {
  address 10.1.1.3/32 {
    destination 10.1.1.2;
  }
}
}
}
t1-5/1/0 {
  unit 0 {
    dlc1 16;
    encapsulation multilink-frame-relay-end-to-end;
    family mlfr-end-to-end {
      bundle ml-1/0/0.1;
    }
  }
}
t1-5/1/1 {
  unit 0 {
    dlc1 17;
    encapsulation multilink-frame-relay-end-to-end;
    family mlfr-end-to-end {
      bundle ml-1/0/0.10;
    }
  }
}
t1-5/1/2 {
  unit 0 {
    dlc1 26;
    encapsulation multilink-frame-relay-end-to-end;
    family mlfr-end-to-end {
      bundle ml-1/0/0.10;
    }
  }
}
```

- Related Documentation**
- [Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386](#)
  - [encapsulation \(Logical Interface\) on page 1448](#)

---

## Examples: Configuring Link Interfaces

The examples in this section include only the configuration of link interfaces. For information about configuring the constituent interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*

- [Example: Configuring a Link Services Interface with Two Links on page 1411](#)
- [Example: Configuring a Link Services Interface with MLPPP on page 1412](#)
- [Example: Configuring a Link Services Interface with MLFR FRF.15 on page 1413](#)
- [Example: Configuring a Link Services PIC with MLFR FRF.16 on page 1413](#)
- [Example: Configuring Link and Voice Services Interfaces with a Combination of Bundle Types on page 1414](#)

Example: Configuring a Link Services Interface with Two Links

This example uses the MLFR UNI NNI protocol between Router A and Router B and logically connects link services bundles **ls-1/1/0.3** and **ls-0/0/0.10**, as specified in [Table 42 on page 1411](#).

Table 42: Link Services Bundle

Router A	Router B
t1-0/1/0 (ls-1/1/0:3)	t1-0/3/0 (ls-0/0/0:10)
t1-0/1/1 (ls-1/1/0:3)	t1-0/3/1 (ls-0/0/0:10)

For LMI to work properly, you must configure one router to be a DCE.

Configuration on Router A

[edit interfaces]  
ls-1/1/0:3 {  
 dce;  
 encapsulation multilink-frame-relay-uni-nni;  
 unit 0 {  
 dlc1 16;  
 family inet {  
 address 10.3.3.1/32 {  
 destination 10.3.3.2;  
 }  
 }  
 }  
}  
t1-0/1/0 {  
 encapsulation multilink-frame-relay-uni-nni;  
 unit 0 {  
 family mlfr-uni-nni {  
 bundle ls-1/1/0:3;  
 }  
 }  
}  
t1-0/1/1 {  
 encapsulation multilink-frame-relay-uni-nni;  
 unit 0 {  
 family mlfr-uni-nni {  
 bundle ls-1/1/0:3;  
 }  
 }  
}

Configuration on Router B

[edit interfaces]  
ls-0/0/0:10 {  
 encapsulation multilink-frame-relay-uni-nni;  
 unit 0 {  
 dlc1 16;  
 family inet {  
 address 10.3.3.2/32 {  
 destination 10.3.3.1;  
 }  
 }  
 }  
}

```
    }  
  }  
}  
t1-0/3/0 {  
  encapsulation multilink-frame-relay-uni-nni;  
  unit 0 {  
    family mlfr-uni-nni {  
      bundle ls-0/0/0:10;  
    }  
  }  
}  
t1-0/3/1 {  
  encapsulation multilink-frame-relay-uni-nni;  
  unit 0 {  
    family mlfr-uni-nni {  
      bundle ls-0/0/0:10;  
    }  
  }  
}
```

- Related Documentation**
- [encapsulation \(Physical Interface\) on page 1449](#)
  - [Configuring Link Services Physical Interfaces on page 1397](#)

### Example: Configuring a Link Services Interface with MLPPP

```
[edit interfaces]  
t1-0/0/0 {  
  encapsulation ppp;  
  unit 0 {  
    family mlppp {  
      bundle ls-0/3/0.0;  
    }  
  }  
}  
t1-0/0/1 {  
  encapsulation ppp;  
  unit 0 {  
    family mlppp {  
      bundle ls-0/3/0.0;  
    }  
  }  
}  
ls-0/3/0 {  
  unit 0 {  
    encapsulation multilink-ppp;  
    family inet {  
      address 10.16.1.2/32 {  
        destination 10.16.1.1;  
      }  
    }  
    family iso;  
    family inet6 {  
      address 2001:DB8:1:2/126;  
    }  
  }  
}
```

```

    }
  }
}

```

- Related Documentation**
- [Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386](#)
  - [encapsulation \(Logical Interface\) on page 1448](#)

### Example: Configuring a Link Services Interface with MLFR FRF.15

```

[edit interfaces]
t1-0/0/0 {
  encapsulation frame-relay;
  unit 0 {
    dlci 16;
    family mlfr-end-to-end {
      bundle ls-0/3/0.0;
    }
  }
}
t1-0/0/1 {
  encapsulation frame-relay;
  unit 0 {
    dlci 16;
    family mlfr-end-to-end {
      bundle ls-0/3/0.0;
    }
  }
}
ls-0/3/0 {
  unit 0 {
    encapsulation multilink-frame-relay-end-to-end;
    family inet {
      address 10.16.1.2/32 {
        destination 10.16.1.1;
      }
    }
    family iso;
    family inet6 {
      address 2001:DB8:1:2/12;
    }
  }
}

```

- Related Documentation**
- [encapsulation \(Logical Interface\) on page 1448](#)

### Example: Configuring a Link Services PIC with MLFR FRF.16

```

[edit chassis]
fpc 1 {
  pic 2 {
    mlfr-uni-nni-bundles 5;
  }
}

```

```
[edit interfaces]
t1-0/0/0 {
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    family mlfr-uni-nni {
      bundle ls-1/2/0:0;
    }
  }
}
t1-0/0/1 {
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    family mlfr-uni-nni {
      bundle ls-1/2/0:0;
    }
  }
}
ls-1/2/0:0 {
  dce;
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    dlci 26;
    family inet {
      address 10.26.1.1/32 {
        destination 10.26.1.2;
      }
    }
  }
}
```

- Related Documentation**
- [Configuring Link Services Physical Interfaces on page 1397](#)
  - [encapsulation \(Physical Interface\) on page 1449](#)

### Example: Configuring Link and Voice Services Interfaces with a Combination of Bundle Types

```
[edit chassis]
fpc 1 {
  pic 3 {
    mlfr-uni-nni-bundles 4;
  }
}
[edit interfaces]
t1-0/2/0:0 {
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    family mlfr-uni-nni {
      bundle ls-1/3/0:0;
    }
  }
}
t1-0/2/0:1 {
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    family mlfr-uni-nni {
```

```

        bundle ls-1/3/0:0;
    }
}
}
t1-0/2/0:5 {
    unit 0 {
        family mlppp {
            bundle ls-1/3/0.2;
        }
    }
}
t1-0/2/0:6 {
    unit 0 {
        family mlppp {
            bundle ls-1/3/0.2;
        }
    }
}
t1-0/2/0:7 {
    encapsulation frame-relay;
    unit 0 {
        dlci 20;
        family mlfr-end-to-end {
            bundle ls-1/3/0.1;
        }
    }
}
t1-0/2/0:8 {
    encapsulation frame-relay;
    unit 0 {
        dlci 20;
        family mlfr-end-to-end {
            bundle ls-1/3/0.1;
        }
    }
}
t1-0/2/0:10 {
    no-keepalives;
    encapsulation ppp;
    unit 0 {
        family mlppp {
            bundle lsq-1/1/0.0;
        }
    }
}
t3-1/0/0 {
    no-keepalives;
    encapsulation ppp;
    unit 0 {
        family mlppp {
            bundle lsq-1/1/0.2;
        }
    }
}
lsq-1/1/0 {
    unit 0 {

```

```
encapsulation multilink-ppp;
compression {
  rtp {
    f-max-period 100;
    queues [ q1 q2 ];
    port minimum 2000 maximum 6000;
  }
}
family inet {
  address 10.5.5.5/24;
}
}
unit 1 {
  encapsulation multilink-ppp;
  compression {
    rtp {
      port minimum 2000 maximum 6000;
    }
  }
  family inet {
    address 10.6.6.1/24;
  }
}
unit 2 {
  encapsulation multilink-ppp;
  compression {
    rtp {
      port minimum 2000 maximum 6000;
    }
  }
  family inet {
    address 10.9.9.1/24;
  }
}
}
t1-1/2/0 {
  no-keepalives;
  unit 0 {
    family mlppp {
      bundle lsq-1/1/0.1;
    }
  }
}
ls-1/3/0 {
  unit 1 {
    encapsulation multilink-frame-relay-end-to-end;
    family inet {
      address 10.1.4.1/24;
    }
  }
  unit 2 {
    encapsulation multilink-ppp;
    family inet {
      address 10.7.4.1/24;
    }
  }
}
```

```

}
ls-1/3/0:0 {
  encapsulation multilink-frame-relay-uni-nni;
  mlfr-uni-nni-bundle-options {
    debug-flags 15;
  }
  unit 0 {
    dlc1 20;
    family inet {
      address 10.5.4.1/24;
    }
  }
}
[edit routing-options]
static {
  route 10.12.12.0/24 next-hop 10.1.1.9;
}

```

On Router B:

```

[edit chassis]
fpc 1 {
  pic 3 {
    mlfr-uni-nni-bundles 4;
  }
}
[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family inet {
      address 10.1.1.1/24;
    }
  }
}
so-0/1/1 {
  encapsulation ppp;
  unit 0 {
    family inet {
      address 10.7.7.7/24;
    }
  }
}
t1-0/2/0:0 {
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    family mlfr-uni-nni {
      bundle ls-1/3/0:0;
    }
  }
}
t1-0/2/0:1 {
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    family mlfr-uni-nni {
      bundle ls-1/3/0:0;
    }
  }
}

```

```
    }  
  }  
  t1-0/2/0:5 {  
    no-keepalives;  
    unit 0 {  
      family mlppp {  
        bundle ls-1/3/0.2;  
      }  
    }  
  }  
  }  
  t1-0/2/0:6 {  
    no-keepalives;  
    unit 0 {  
      family mlppp {  
        bundle ls-1/3/0.2;  
      }  
    }  
  }  
  }  
  t1-0/2/0:7 {  
    dce;  
    encapsulation frame-relay;  
    unit 0 {  
      dlci 20;  
      family mlfr-end-to-end {  
        bundle ls-1/3/0.1;  
      }  
    }  
  }  
  }  
  t1-0/2/0:8 {  
    dce;  
    encapsulation frame-relay;  
    unit 0 {  
      dlci 20;  
      family mlfr-end-to-end {  
        bundle ls-1/3/0.1;  
      }  
    }  
  }  
  }  
  t1-0/2/0:10 {  
    no-keepalives;  
    encapsulation ppp;  
    unit 0 {  
      family mlppp {  
        bundle lsq-1/1/0.0;  
      }  
    }  
  }  
  }  
  t3-0/3/0 {  
    no-keepalives;  
    encapsulation ppp;  
    unit 0 {  
      family mlppp {  
        bundle lsq-1/1/0.2;  
      }  
    }  
  }  
}
```

```
ge-1/0/0 {
  unit 0 {
    family inet {
      address 10.2.2.1/24;
    }
  }
}
lsq-1/1/0 {
  unit 0 {
    compression {
      rtp {
        port minimum 2000 maximum 6000;
      }
    }
    family inet {
      address 10.5.5.1/24;
    }
  }
  unit 1 {
    encapsulation multilink-ppp;
    compression {
      rtp {
        port minimum 16384 maximum 20102;
      }
    }
    family inet {
      address 10.3.4.1/24;
    }
  }
  unit 2 {
    encapsulation multilink-ppp;
    compression {
      rtp {
        port minimum 2000 maximum 6000;
      }
    }
    family inet {
      address 10.9.9.9/24;
    }
  }
}
t1-1/2/2 {
  no-keepalives;
  unit 0 {
    family mlppp {
      bundle ls-1/3/0.1;
    }
  }
}
t1-1/2/3 {
  no-keepalives;
  unit 0 {
    family mlppp {
      bundle lsq-1/1/0.1;
    }
  }
}
```

```
}
ls-1/3/0 {
  unit 1 {
    encapsulation multilink-frame-relay-end-to-end;
    family inet {
      address 10.1.4.4/24;
    }
    family iso;
  }
  unit 2 {
    encapsulation multilink-ppp;
    family inet {
      address 10.7.4.4/24;
    }
  }
}
ls-1/3/0:0 {
  dce;
  encapsulation multilink-frame-relay-uni-nni;
  unit 0 {
    dlci 20;
    family inet {
      address 10.5.4.4/24;
    }
  }
}
[edit routing-options]
static {
  route 10.12.12.0/24 next-hop 10.3.4.4;
}
```

- Related Documentation**
- [Configuring Link Services Physical Interfaces on page 1397](#)
  - [encapsulation \(Physical Interface\) on page 1449](#)

---

## Example: Configuring an MLPPP Bundle

This example shows how to configure an MLPPP bundle to increase traffic bandwidth.

- [Requirements on page 1420](#)
- [Overview on page 1420](#)
- [Configuration on page 1421](#)
- [Verification on page 1423](#)

### Requirements

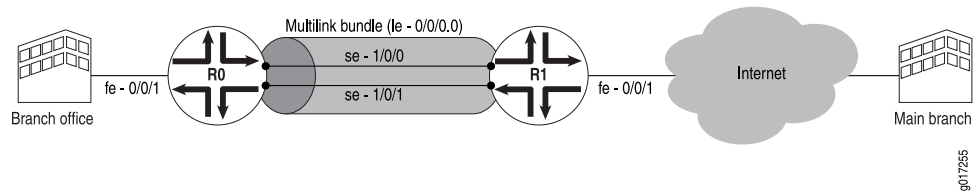
Before you begin, you should have two MX Series routers (MX240, MX480, or MX960 routers) configured with at least two serial interfaces that communicate over serial links.

### Overview

In this example, you create the MLPPP bundle lsq-0/0/0.0 at the logical unit level of the link services interface lsq-0/0/0 on the MX Series routers R0 and R1. You then add the

two serial interfaces se-1/0/0 and se-1/0/1 as constituent links to the multilink bundle. In [Figure 27 on page 1421](#), your company's branch office is connected to its main branch using routers R0 and R1. You transmit data and voice traffic on two low-speed 1-Mbps serial links. To increase bandwidth, you configure MLPPP and join the two serial links se-1/0/0 and se-1/0/1 into the multilink bundle lsq-0/0/0.0. Then you configure LFI and CoS on R0 and R1 to enable them to transmit voice packets ahead of data packets.

**Figure 27: Configuring MLPPP and LFI on Serial Links**



## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

For device R0

```
set interfaces lsq-0/0/0 unit 0 family inet address 10.0.0.10/24
set interfaces se-1/0/0 unit 0 family mlppp bundle lsq-0/0/0.0
set interfaces se-1/0/1 unit 0 family mlppp bundle lsq-0/0/0.0
set interfaces se-1/0/0 serial-options clocking-mode dce clock-rate 2.0mhz
set interfaces se-1/0/1 serial-options clocking-mode dce clock-rate 2.0mhz
```

For device R1

```
set interfaces lsq-0/0/0 unit 0 family inet address 10.0.0.9/24
set interfaces se-1/0/0 unit 0 family mlppp bundle lsq-0/0/0.0
set interfaces se-1/0/1 unit 0 family mlppp bundle lsq-0/0/0.0
```

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure MLPPP bundle:

1. Create an interface on both the routers.  

```
[edit]
user@host# edit interfaces lsq-0/0/0 unit 0
```
2. Configure a family inet and define the IP address on device R0.  

```
[edit interfaces lsq-0/0/0 unit 0]
user@host# set family inet address 10.0.0.10/24
```
3. Configure a family inet and define the IP address on device R1.  

```
[edit interfaces lsq-0/0/0 unit 0]
user@host# set family inet address 10.0.0.9/24
```

4. Specify the names of the constituent links to be added to the multilink bundle on both the routers.

```
[edit interfaces]
user@host# edit se-1/0/0 unit 0
user@host# set family mlppp bundle lsq-0/0/0.0
[edit interfaces]
user@host# edit se-1/0/1 unit 0
user@host# set family mlppp bundle lsq-0/0/0.0
```

5. Set the serial options to the same values for both interfaces on R0.



**NOTE:** R0 is set as a DCE device. The serial options are not set for interfaces on R1. You can set the serial options according to your network setup.

```
[edit interfaces]
user@host# set se-1/0/0 serial-options clocking-mode dce clock-rate 2.0mhz
user@host# set se-1/0/1 serial-options clocking-mode dce clock-rate 2.0mhz
```

**Results** From configuration mode, confirm your configuration by entering the **show interfaces lsq-0/0/0**, **show interfaces se-1/0/0**, and **show interfaces se-1/0/1** commands for R0 and R1. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
For device R0
[edit]
user@host# show interfaces lsq-0/0/0
family inet {
  address 10.0.0.10/24;
}
[edit]
user@host# show interfaces se-1/0/0
clocking-mode dce;
clock-rate 2.0mhz;
}
unit 0 {
  family mlppp {
    bundle lsq-0/0/0.0;
  }
}
[edit]
user@host# show interfaces se-1/0/1
serial-options {
  clocking-mode dce;
  clock-rate 2.0mhz;
}
unit 0 {
  family mlppp {
    bundle lsq-0/0/0.0;
  }
}
```

```

    }
For device R1
[edit]
user@host# show interfaces lsq-0/0/0
    family inet {
        address 10.0.0.9/24;
    }
}
[edit]
user@host# show interfaces se-1/0/0
    unit 0 {
        family mlppp {
            bundle lsq-0/0/0.0;
        }
    }
}
[edit]
user@host# show interfaces se-1/0/1
    unit 0 {
        family mlppp {
            bundle lsq-0/0/0.0;
        }
    }
}

```

If you are done configuring the router, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly:

- [Verifying the MLPPP Bundle on page 1423](#)

### Verifying the MLPPP Bundle

**Purpose** Verify that the constituent links are added to the bundle correctly.

**Action** From operational mode, enter the **show interfaces lsq-0/0/0 statistics** command.

**Related Documentation**

- [Link and Multilink Services Overview on page 1371](#)
- [Multilink Interfaces on Channelized MICs Overview on page 1379](#)
- [Understanding MLPPP Bundles and Link Fragmentation and Interleaving \(LFI\) on Serial Links on page 1381](#)
- [Example: Configuring Link Interfaces on Channelized MICs on page 1430](#)
- [Example: Configuring Multilink Frame Relay FRF.15 on page 1424](#)
- [Example: Configuring Multilink Frame Relay FRF.16 on page 1427](#)

## Example: Configuring Multilink Frame Relay FRF.15

---

This example shows how to configure MLFR FRF.15 for additional bandwidth, load balancing, and redundancy by aggregating low-speed links such as T1, E1, and serial links.

- [Requirements on page 1424](#)
- [Overview on page 1424](#)
- [Configuration on page 1424](#)
- [Verification on page 1426](#)

### Requirements

Before you begin, you should have two MX Series 3D Universal Edge Routers (MX240, MX480, or MX960 routers) configured with at least two serial interfaces that communicate over serial links.

### Overview

In this example, you aggregate two T1 links to create the MLFR FRF.15 bundle on two MX Series routers, R0 and R1, and set the interface to lsq-0/0/0. You configure a logical unit on the lsq-0/0/0 interface and set the family type to **inet** with address 10.0.0.4/24. Then you configure an IP address for the multilink bundle on the unit level of the interface.

You define the multilink bundle as an MLFR FRF.15 bundle by specifying the MLFR end-to-end encapsulation type. You specify the names of the constituent links to be added to the multilink bundle as t1-2/0/0 and t1-2/0/1 and set the encapsulation type to **frame-relay**. You then define R0 as a DCE device and R1 as a DTE device. You set the DLCI value to 100 (range is from 16 through 1022). Finally, you set the multilink bundle to lsq-0/0/0.0.

### Configuration

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

For device R0

```
set interfaces lsq-0/0/0 unit 0 family inet address 10.0.0.4/24
set interfaces lsq-0/0/0 unit 0 encapsulation multilink-frame-relay-end-to-end
set interfaces t1-2/0/0 encapsulation frame-relay
set interfaces t1-2/0/1 encapsulation frame-relay
set interfaces lsq-0/0/0 dce
set interfaces lsq-0/0/0 unit 0 dlci 100 family mlfr-end-to-end bundle lsq-0/0/0.0
```

For device R1

```
set interfaces lsq-0/0/0 unit 0 family inet address 10.0.0.5/24
set interfaces lsq-0/0/0 unit 0 encapsulation multilink-frame-relay-end-to-end
set interfaces t1-2/0/0 encapsulation frame-relay
set interfaces t1-2/0/1 encapsulation frame-relay
set interfaces lsq-0/0/0 unit 0 dlci 100 family mlfr-end-to-end bundle lsq-0/0/0.0
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the MLFR FRF.15 bundle:

1. Create an interface on both the routers.  

```
[edit]
user@host# edit interfaces lsq-0/0/0 unit 0
```
2. Set a logical unit on the interface and define the family type for the routers R0 and R1.  

```
[edit interfaces lsq-0/0/0 unit 0]
user@host# set family inet address 10.0.0.4/24
user@host# set family inet address 10.0.0.5/24
```
3. Define the multilink bundle as an MLFR FRF.15 bundle.  

```
[edit interfaces lsq-0/0/0 unit 0]
user@host# set encapsulation multilink-frame-relay-end-to-end
```
4. Specify the names of the constituent links to be added to the multilink bundle.  

```
[edit interfaces]
user@host# set t1-2/0/0 encapsulation frame-relay
user@host# set t1-2/0/1 encapsulation frame-relay
```
5. Define the router R0 as a DCE device.  

```
[edit interfaces]
user@host# edit lsq-0/0/0
user@host# set dce
```
6. Specify the DLCI as well as the multilink bundle to which the interface is to be added.  

```
[edit interfaces lsq-0/0/0]
user@host# set unit 0 dlci 100 family mlfr-end-to-end bundle lsq-0/0/0.0
```

**Results** From configuration mode, confirm your configuration by entering the **show interfaces lsq-0/0/0**, **show interfaces t1-2/0/0**, and **show interfaces t1-2/0/1** commands for R0 and R1. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
For device R0
[edit]
user@host# show interfaces lsq-0/0/0
dce;
unit 0 {
  encapsulation multilink-frame-relay-end-to-end;
  dlci 100;
  family inet {
    address 10.0.0.4/24;
  }
  family mlfr-end-to-end {
    bundle lsq-0/0/0.0;
  }
}
```

```
[edit]
user@host#show interfaces t1-2/0/0
encapsulation frame-relay;
[edit]
user@host# show interfaces t1-2/0/1
encapsulation frame-relay;

For device R1
[edit]
user@host# show interfaces lsq-0/0/0
unit 0 {
encapsulation multilink-frame-relay-end-to-end;
    dlc1 100;
    family inet {
address 10.0.0.5/24;
    }
family mlfr-end-to-end {
    bundle lsq-0/0/0.0;
    }
}
[edit]
user@host# show interfaces t1-2/0/0
encapsulation frame-relay;
[edit]
user@host# show interfaces t1-2/0/1
encapsulation frame-relay;
```

If you are done configuring the router, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly:

- [Verifying the MLFR FRF.15 Configuration on page 1426](#)

---

### Verifying the MLFR FRF.15 Configuration

**Purpose** Verify the MLFR FRF.15 configuration.

**Action** From operational mode, enter the **show interfaces** command.

**Related Documentation**

- [Link and Multilink Services Overview on page 1371](#)
- [Multilink Interfaces on Channelized MICs Overview on page 1379](#)
- [Understanding MLPPP Bundles and Link Fragmentation and Interleaving \(LFI\) on Serial Links on page 1381](#)
- [Example: Configuring Link Interfaces on Channelized MICs on page 1430](#)
- [Example: Configuring an MLPPP Bundle on page 1420](#)
- [Example: Configuring Multilink Frame Relay FRF.16 on page 1427](#)

## Example: Configuring Multilink Frame Relay FRF.16

This example shows how to configure MLFR FRF.16 for additional bandwidth, load balancing, and redundancy.

- [Requirements on page 1427](#)
- [Overview on page 1427](#)
- [Configuration on page 1427](#)
- [Verification on page 1430](#)

### Requirements

Before you begin, you should have two MX Series 3D Universal Edge Routers configured with at least two serial interfaces that communicate over serial links.

### Overview

In this example, you aggregate two T1 interfaces to create an MLFR FRF.16 bundle on two MX Series, R0 and R1. You configure the chassis interface and specify the number of MLFR FRF.16 bundles to be created on the interface. You then specify the channel to be configured as a multilink bundle and create interface lsq-0/0/0:0. You set the multilink bundle as an MLFR FRF.16 bundle by specifying the MLFR UNI NNI encapsulation type.

Then you define R0 as a DCE device and R1 as a DTE device. You configure a logical unit on the multilink bundle lsq-0/0/0:0, and set the family type to inet. You then assign a DLCI of 400 and an IP address of 10.0.0.10/24 to the multilink bundle. You create the T1 interfaces, t1-2/0/0 and t1-2/0/1, that are to be added as constituent links to the multilink bundle and define the Frame Relay encapsulation type. Finally, you set the multilink bundle to lsq-0/0/0:0.

### Configuration

#### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
For device R0
set chassis fpc 0 pic 0 mlfr-uni-nni-bundles 1
set interfaces lsq-0/0/0:0 encapsulation multilink-frame-relay-uni-nni
set interfaces lsq-0/0/0 dce
set interfaces lsq-0/0/0 unit 0 dlci 400 family inet address 10.0.0.10/24
set interfaces t1-2/0/0 encapsulation multilink-frame-relay-uni-nni
set interfaces t1-2/0/1 encapsulation multilink-frame-relay-uni-nni
set interfaces t1-2/0/0 unit 0 family mlfr-uni-nni bundle lsq-0/0/0:0
set interfaces t1-2/0/1 unit 0 family mlfr-uni-nni bundle lsq-0/0/0:0
For device R1
set chassis fpc 0 pic 0 mlfr-uni-nni-bundles 1
set interfaces lsq-0/0/0:0 encapsulation multilink-frame-relay-uni-nni
set interfaces lsq-0/0/0 unit 0 dlci 400 family inet address 10.0.0.9/24
set interfaces t1-2/0/0 encapsulation multilink-frame-relay-uni-nni
set interfaces t1-2/0/1 encapsulation multilink-frame-relay-uni-nni
```

```
set interfaces t1-2/0/0 unit 0 family mlfr-uni-nni bundle lsq-0/0/0:0
set interfaces t1-2/0/1 unit 0 family mlfr-uni-nni bundle lsq-0/0/0:0
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure an MLFR FRF.16 bundle:

1. Configure a chassis interface.

```
[edit]
user@host# edit chassis
```

2. Specify the number of MLFR bundles.

```
[edit chassis]
user@host# set fpc 0 pic 0 mlfr-uni-nni-bundles 1
```

3. Create an interface.

```
[edit]
user@host# edit interfaces lsq-0/0/0:0
```

4. Specify the MLFR encapsulation type.

```
[edit interfaces lsq-0/0/0:0]
user@host# set encapsulation multilink-frame-relay-uni-nni
```

5. Set the router R0 as a DCE device.

```
[edit]
user@host# edit interfaces lsq-0/0/0
user@host# set dce
```

6. Specify a logical unit on the multilink bundle and set the family type.

```
[edit interfaces lsq-0/0/0]
user@host# set unit 0 dlci 400 family inet address 10.0.0.10/24
```

7. Create the T1 interfaces and set the Frame Relay encapsulation.

```
[edit interfaces]
user@host# set t1-2/0/0 encapsulation multilink-frame-relay-uni-nni
user@host# set t1-2/0/1 encapsulation multilink-frame-relay-uni-nni
```

8. Specify the multilink bundle to which the interface is to be added as a constituent link on device R0.

```
[edit interfaces t1-2/0/0]
user@host# set unit 0 family mlfr-uni-nni bundle lsq-0/0/0:0
```

9. Specify the multilink bundle to which the interface is to be added as a constituent link on device R1.

```
[edit interfaces t1-2/0/1]
user@host# set unit 0 family mlfr-uni-nni bundle lsq-0/0/0:0
```

**Results** From configuration mode, confirm your configuration by entering the **show chassis**, **show interfaces lsq-0/0/0**, **show interfaces lsq-0/0/0:0**, **show interfaces t1-2/0/0**, and **show interfaces t1-2/0/1** commands for the routers R0 and R1. If the output does not display

the intended configuration, repeat the configuration instructions in this example to correct it.

```

For device R0
[edit]
user@host# show chassis
fpc 0 {
pic 0 {
mlfr-uni-nni-bundles 1;
}
}
[edit]
user@host# show interfaces lsq-0/0/0
dce;
unit 0 {
dlci 400;
family inet {
address 10.0.0.10/24;
}
}
[edit]
user@host# show interfaces lsq-0/0/0:0
encapsulation multilink-frame-relay-uni-nni;
[edit]
user@host# show interfaces t1-2/0/0
encapsulation multilink-frame-relay-uni-nni;
unit 0 {
family mlfr-uni-nni {
bundle lsq-0/0/0:0;
}
}
[edit]
user@host# show interfaces t1-2/0/1
encapsulation multilink-frame-relay-uni-nni;
unit 0 {
family mlfr-uni-nni {
bundle lsq-0/0/0:0;
}
}

For device R1
[edit]
user@host# show chassis
unit 0 {
dlci 400;
family inet {
address 10.0.0.9/24;
}
}
[edit]
user@host# show interfaces lsq-0/0/0:0
encapsulation multilink-frame-relay-uni-nni;
[edit]
user@host# show interfaces t1-2/0/0
encapsulation multilink-frame-relay-uni-nni;
unit 0 {

```

```
        family mlfr-uni-nni {
        bundle lsq-0/0/0:0;
        }
    }
[edit]
user@host# show interfaces t1-2/0/1
encapsulation multilink-frame-relay-uni-nni;
unit 0 {
    family mlfr-uni-nni {
    bundle lsq-0/0/0:0;
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

Confirm that the configuration is working properly:

- [Verifying the MLFR FRF.16 Configuration on page 1430](#)

---

### Verifying the MLFR FRF.16 Configuration

**Purpose** Verify the MLFR FRF.16 configuration.

**Action** From operational mode, enter the **show interfaces** command.

**Related Documentation**

- [Link and Multilink Services Overview on page 1371](#)
- [Multilink Interfaces on Channelized MICs Overview on page 1379](#)
- [Understanding MLPPP Bundles and Link Fragmentation and Interleaving \(LFI\) on Serial Links on page 1381](#)
- [Example: Configuring Link Interfaces on Channelized MICs on page 1430](#)
- [Example: Configuring an MLPPP Bundle on page 1420](#)
- [Example: Configuring Multilink Frame Relay FRF.15 on page 1424](#)

---

## Example: Configuring Link Interfaces on Channelized MICs

- [Requirements on page 1430](#)
- [Overview on page 1431](#)
- [Configuration on 4-port Channelized SONET/SDH OC3/STM1 \(Multi-Rate\) MIC with SFP on page 1431](#)
- [Verification on page 1439](#)

## Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.1 or later for MX240, MX480, and MX960 routers

- One MX240, MX480, or MX960 router

## Overview

This example provides information about configuring the link interfaces on the following channelized MICs:

- 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP (MIC-3D-4CHOC3-2CHOC12)
- 8-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP (MIC-3D-8CHOC3-4CHOC12)
- 8-port Channelized DS3/E3 MIC (MIC-3D-8CHDS3-E3-B)

You need to first partition each port on the MICs to configure the link interfaces T1, T3, and DS, and then you configure the link interfaces for bundles. An MLPPP bundle involves "bundling" multiple T1/T3/DS interfaces into a single, logical interface that uses only one IP address. For more information about MLPPP bundles, see ["Understanding MLPPP Bundles and Link Fragmentation and Interleaving \(LFI\) on Serial Links" on page 1381](#). Similarly, you can partition the ports to configure the MICs to the E1/E3 interfaces by setting the framing mode to SDH.

For more information about multilink-based protocols on MX240, MX480, and MX960 routers with Multiservices DPC, see ["Multilink Interfaces on Channelized MICs Overview" on page 1379](#).

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.



**NOTE:** You can set the values for each parameter according to your requirement. The values given in this example are for illustration purposes only.

## Configuration on 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP

To partition each port on the MIC and configure the link interfaces T1, T3, and DS on it and to configure the link interfaces for bundles, perform the following tasks:

- [Partitioning Ports on the Channelized MICs and Configuring the Link Interfaces T1, T3, and DS on page 1433](#)
- [Configuring MLPPP, MLFR FRF.15, and MLFR FRF.16 on Link Interfaces for Bundles on page 1435](#)
- [Results on page 1436](#)

### CLI Quick Configuration

To quickly configure synchronization on the aforementioned routers, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

[edit]

```
set interfaces coc12-5/2/0 partition 1 interface-type coc1
set interfaces coc12-5/2/0 partition 1 oc-slice 1
set interfaces coc12-5/2/0 partition 2 oc-slice 2 interface-type coc1
set interfaces coc12-5/2/0 partition 3 oc-slice 3 interface-type coc1
set interfaces coc1-5/2/0:1 no-partition interface-type t3
set interfaces coc1-5/2/0:3 no-partition interface-type t3
set interfaces coc1-5/2/0:2 partition 1 interface-type ct1
set interfaces coc1-5/2/0:2 partition 2 interface-type t1
set interfaces coc1-5/2/0:2 partition 3 interface-type ct1
set interfaces coc1-5/2/0:2 partition 4 interface-type t1
set interfaces ct1-5/2/0:2:1 partition 1 timeslots 1 interface-type ds
set interfaces ct1-5/2/0:2:1 partition 2 timeslots 2 interface-type ds
set interfaces ct3-2/0/0 no-partition interface-type t3
set interfaces ct3-2/0/0 partition 1 interface-type t1
set interfaces ct3-2/0/0 partition 2 interface-type t1
set interfaces ct3-2/0/0 partition 3 interface-type t1
set interfaces ct3-2/0/0 partition 4 interface-type ct1
set interfaces ct1-5/2/0:2:1 partition 1 timeslots 1 interface-type ds
set interfaces t1-5/2/0:2:2 unit 0 family mlppp bundle rlsq0.1
set interfaces ds-5/2/0:2:1:1 unit 0 family mlppp bundle rlsq0.0
set interfaces ds-5/2/0:2:1:2 unit 0 family mlppp bundle rlsq0.0
set interfaces t3-5/2/0:3 unit 0 family mlppp bundle rlsq0.2
set interfaces t3-5/2/0:1 unit 0 family mlppp bundle rlsq0.2
set interfaces t1-5/2/0:2:2 encapsulation multilink-frame-relay-uni-nni unit 0 family
mlfr-uni-nni bundle rlsq0:0
set interfaces t1-5/2/0:2:4 encapsulation multilink-frame-relay-uni-nni unit 0 family
mlfr-uni-nni bundle rlsq0:0
set interfaces ds-5/2/0:2:1:1 encapsulation multilink-frame-relay-uni-nni unit 0 family
mlfr-uni-nni bundle rlsq0:0
set interfaces ds-5/2/0:2:1:2 encapsulation multilink-frame-relay-uni-nni unit 0 family
mlfr-uni-nni bundle rlsq0:0
set interfaces t1-5/2/0:2:2 encapsulation frame-relay unit 0 dlci 10 family mlfr-end-to-end
bundle rlsq0.0
set interfaces t1-5/2/0:2:4 encapsulation frame-relay unit 0 dlci 11 family mlfr-end-to-end
bundle rlsq0.0
set interfaces ds-5/2/0:2:1:1 encapsulation frame-relay unit 0 dlci 10 family
mlfr-end-to-end bundle rlsq0.0
set interfaces ds-5/2/0:2:1:2 encapsulation frame-relay unit 0 dlci 11 family
mlfr-end-to-end bundle rlsq0.0
set interfaces t3-5/2/0:1 encapsulation frame-relay unit 0 dlci 11 family mlfr-end-to-end
bundle rlsq0.1
set interfaces t3-5/2/0:3 encapsulation frame-relay unit 0 dlci 10 family mlfr-end-to-end
bundle rlsq0.1
```

## Partitioning Ports on the Channelized MICs and Configuring the Link Interfaces T1, T3, and DS

### Step-by-Step Procedure

To partition each port on the channelized MICs:

1. Configure the **coc12-5/2/0** interface by setting the **partition** option to 1 with the sublevel interface type set to **coc1**.  

```
[edit interfaces]
user@host# set coc12-5/2/0 partition 1 interface-type coc1
```
2. Configure the **coc12-5/2/0** interface with the OC-slice range (OC-slice range specifies the bandwidth size required for the interface type you are configuring) set to 1.  

```
[edit interfaces]
user@host# set coc12-5/2/0 partition 1 oc-slice 1
```
3. Configure the **coc12-5/2/0** interface by setting the **partition** option to 2 with the sublevel interface type set to **coc1** and the OC-slice range set to 2.  

```
[edit interfaces]
user@host# set coc12-5/2/0 partition 2 oc-slice 2 interface-type coc1
```
4. Configure the **coc12-5/2/0** interface by setting the **partition** option to 3 with the sublevel interface type set to **coc1** and the OC-slice range set to 3.  

```
[edit interfaces]
user@host# set coc12-5/2/0 partition 3 oc-slice 3 interface-type coc1
```
5. Configure the **coc1-5/2/0:1** interface as a clear channel by setting the **no-partition** option for the sublevel interface type **t3**. (A clear channel consolidates the entire bandwidth of a channelized interface into a single unpartitioned stream that looks like a standard interface.)  

```
[edit interfaces]
user@host# set coc1-5/2/0:1 no-partition interface-type t3
```
6. Configure the **coc1-5/2/0:3** interface as a clear channel by setting the **no-partition** option for the sublevel interface type **t3**.  

```
[edit interfaces]
user@host# set coc1-5/2/0:3 no-partition interface-type t3
```
7. Configure the **coc1-5/2/0:2** interface by setting the **partition** option to 1 and 3 with the sublevel interface type set to **ct1**. Configure the **coc1-5/2/0:2** interface by setting the **partition** option to 2 and 4 with the sublevel interface type set to **t1**.  

```
[edit interfaces]
user@host# set coc1-5/2/0:2 partition 1 interface-type ct1
user@host# set coc1-5/2/0:2 partition 2 interface-type t1
user@host# set coc1-5/2/0:2 partition 3 interface-type ct1
user@host# set coc1-5/2/0:2 partition 4 interface-type t1
```
8. Configure the **ct1-5/2/0:2:1** interface by setting the **partition** option to 1 and 2 with the sublevel interface type set to **ds**. Configure the time slots for the partitions.  

```
[edit interfaces]
user@host# set ct1-5/2/0:2:1 partition 1 timeslots 1 interface-type ds
user@host# set ct1-5/2/0:2:1 partition 2 timeslots 2 interface-type ds
```

9. Configure a clear channel on the channelized interface **ct3-2/0/0** by setting the **no-partition** option to the sublevel interface type **t3** (a clear channel consolidates the entire bandwidth of a channelized interface into a single unpartitioned stream that looks like a standard interface).

```
[edit interfaces]
user@host# set ct3-2/0/0 no-partition interface-type t3
```

10. Configure a clear channel on the channelized interface **ct3-2/0/0** by setting the **partition** option to **1**, **2**, and **3** with the sublevel interface type **ds**. Configure the **ct3-2/0/0** interface by setting the **partition** option to **4** with the sublevel interface type **ct1**.

```
[edit interfaces]
user@host# set ct3-2/0/0 partition 1 interface-type t1
user@host# set ct3-2/0/0 partition 2 interface-type t1
user@host# set ct3-2/0/0 partition 3 interface-type t1
user@host# set ct3-2/0/0 partition 4 interface-type ct1
```

11. Configure the **ct1-2/0/0:4** interface by setting the **partition** option to **1** and **2** with the sublevel interface type set to **ds**. Configure the time slots for the partitions.

```
[edit interfaces]
user@host# set ct1-5/2/0:2:1 partition 1 timeslots 1 interface-type ds
user@host# set ct1-5/2/0:2:1 partition 2 timeslots 2 interface-type ds
```

**Results** Display the results of partitioning each port on the MIC and configuring the link interfaces T1, T3, and DS:

**Results for CHOC12/3 interfaces**

```
user@host# show interfaces
coc12-5/2/0 {
  partition 1 oc-slice 1 interface-type coc1;
  partition 2 oc-slice 2 interface-type coc1;
  partition 3 oc-slice 3 interface-type coc1;
}
coc1-5/2/0:1 {
  no-partition interface-type t3;
}
coc1-5/2/0:3 {
  no-partition interface-type t3;
}
coc1-5/2/0:2 {
  partition 1 interface-type ct1;
  partition 2 interface-type t1;
  partition 3 interface-type ct1;
  partition 4 interface-type t1;
}
```

**Results for CHDS3 MIC interfaces**

```
user@host# show interfaces
ct1-5/2/0:2:1 {
  partition 1 timeslots 1 interface-type ds;
  partition 2 timeslots 2 interface-type ds;
}
ct3-2/0/0 {
  no-partition interface-type t3;
  partition 1 interface-type t1;
```

```

partition 2 interface-type t1;
partition 3 interface-type t1;
partition 4 interface-type ct1;
}
ct1-2/0/0:4 {
partition 1 timeslots 1 interface-type ds;
partition 2 timeslots 2 interface-type ds;
}

```

### Configuring MLPPP, MLFR FRF.15, and MLFR FRF.16 on Link Interfaces for Bundles

#### Step-by-Step Procedure

To configure MLPPP, MLFR FRF.15, and MLFR FRF.16 on the link interfaces T1, T3, and DS for bundles:

1. Configure the MLPPP encapsulation on the T1 link interfaces **t1-5/2/0:2:2** and **t1-5/2/0:2:4**.  

```

[edit interfaces]
user@host# set t1-5/2/0:2:2 unit 0 family mlppp bundle rlsq0.1
user@host# set t1-5/2/0:2:4 unit 0 family mlppp bundle rlsq0.1

```
2. Configure the MLPPP encapsulation on the DS link interfaces **ds-5/2/0:2:1:1** and **ds-5/2/0:2:1:2**.  

```

[edit interfaces]
user@host# set ds-5/2/0:2:1:1 unit 0 family mlppp bundle rlsq0.0
user@host# set ds-5/2/0:2:1:2 unit 0 family mlppp bundle rlsq0.0

```
3. Configure the MLPPP encapsulation on the T3 link interfaces **t3-5/2/0:3** and **t3-5/2/0:1**.  

```

[edit interfaces]
user@host# set t3-5/2/0:3 unit 0 family mlppp bundle rlsq0.2
user@host# set t3-5/2/0:1 unit 0 family mlppp bundle rlsq0.2

```
4. Configure the MLFR FRF.16 encapsulation on the T1 link interfaces **t1-5/2/0:2:2** and **t1-5/2/0:2:4**.  

```

[edit interfaces]
user@host# set t1-5/2/0:2:2 encapsulation multilink-frame-relay-uni-nni unit 0
family mlfr-uni-nni bundle rlsq0:0
user@host# set t1-5/2/0:2:4 encapsulation multilink-frame-relay-uni-nni unit 0
family mlfr-uni-nni bundle rlsq0:0

```
5. Configure the MLFR FRF.16 encapsulation on the DS link interfaces **ds-5/2/0:2:1:1** and **ds-5/2/0:2:1:2**.  

```

[edit interfaces]
user@host# set ds-5/2/0:2:1:1 encapsulation multilink-frame-relay-uni-nni unit 0
family mlfr-uni-nni bundle rlsq0:0
user@host# set ds-5/2/0:2:1:2 encapsulation multilink-frame-relay-uni-nni unit 0
family mlfr-uni-nni bundle rlsq0:0

```
6. Configure the MLFR FRF.15 encapsulation on the T1 link interfaces **t1-5/2/0:2:2** and **t1-5/2/0:2:4**.  

```

[edit interfaces]
user@host# set t1-5/2/0:2:2 encapsulation frame-relay unit 0 dlci 10 family
mlfr-end-to-end bundle rlsq0:0

```

```
user@host# set t1-5/2/0:2:4 encapsulation frame-relay unit 0 dlci 11 family
mlfr-end-to-end bundle rlsq0.0
```

7. Configure the MLFR FRF.15 encapsulation on the DS link interfaces **ds-5/2/0:2:1:1** and **ds-5/2/0:2:1:2**.

```
[edit interfaces]
user@host# set ds-5/2/0:2:1:1 encapsulation frame-relay unit 0 dlci 10 family
mlfr-end-to-end bundle rlsq0.0
user@host# set ds-5/2/0:2:1:2 encapsulation frame-relay unit 0 dlci 11 family
mlfr-end-to-end bundle rlsq0.0
```

8. Configure the MLFR FRF.15 encapsulation on the T3 link interfaces **t3-5/2/0:1** and **t3-5/2/0:3**.

```
[edit interfaces]
user@host# set t3-5/2/0:1 encapsulation frame-relay unit 0 dlci 11 family
mlfr-end-to-end bundle rlsq0.1
user@host# set t3-5/2/0:3 encapsulation frame-relay unit 0 dlci 10 family
mlfr-end-to-end bundle rlsq0.1
```

## Results

Display the results of the configuration of link interfaces for bundles:

### MLPPP on T1 links

```
user@host# show interfaces
t1-5/2/0:2:2 {
  unit 0 {
    family mlppp {
      bundle rlsq0.1;
    }
  }
}
t1-5/2/0:2:4 {
  unit 0 {
    family mlppp {
      bundle rlsq0.1;
    }
  }
}
```

### MLPPP on DS links

```
user@host# show interfaces
ds-5/2/0:2:1:1 {
  unit 0 {
    family mlppp {
      bundle rlsq0.0;
    }
  }
}
ds-5/2/0:2:1:2 {
  unit 0 {
    family mlppp {
      bundle rlsq0.0;
    }
  }
}
```

**MLPPP on T3 links**

```

user@host# show interfaces
t3-5/2/0:3 {
  unit 0 {
    family mlppp {
      bundle rlsq0.2;
    }
  }
}
t3-5/2/0:1 {
  unit 0 {
    family mlppp {
      bundle rlsq0.2;
    }
  }
}

```

**MLFR FRF.15 on T1 links**

```

user@host# show interfaces
t1-5/2/0:2:2 {
  encapsulation frame-relay;
  unit 0 {
    dlci 10;
    family mlfr-end-to-end {
      bundle rlsq0.0;
    }
  }
}
t1-5/2/0:2:4 {
  encapsulation frame-relay;
  unit 0 {
    dlci 11;
    family mlfr-end-to-end {
      bundle rlsq0.0;
    }
  }
}

```

**MLFR FRF.15 on DS links**

```

user@host# show interfaces
ds-5/2/0:2:1:1 {
  encapsulation frame-relay;
  unit 0 {
    dlci 10;
    family mlfr-end-to-end {
      bundle rlsq0.0;
    }
  }
}
ds-5/2/0:2:1:2 {
  encapsulation frame-relay;
  unit 0 {
    dlci 11;
    family mlfr-end-to-end {
      bundle rlsq0.0;
    }
  }
}

```

<b>MLFR FRF.15 on T3 links</b>	<pre> user@host# show interfaces t3-5/2/0:1 {   encapsulation frame-relay;   unit 0 {     dlci 11;     family mlfr-end-to-end {       bundle rlsq0.1;     }   } } t3-5/2/0:3 {   encapsulation frame-relay;   unit 0 {     dlci 10;     family mlfr-end-to-end {       bundle rlsq0.1;     }   } } </pre>
<b>MLFR FRF.16 on T1 links</b>	<pre> user@host# show interfaces t1-5/2/0:2:2 {   encapsulation multilink-frame-relay-uni-nni;   unit 0 {     family mlfr-uni-nni {       bundle rlsq0:0;     }   } } t1-5/2/0:2:4 {   encapsulation multilink-frame-relay-uni-nni;   unit 0 {     family mlfr-uni-nni {       bundle rlsq0:0;     }   } } </pre>
<b>MLFR FRF.16 on DS links</b>	<pre> user@host# show interfaces ds-5/2/0:2:1:1 {   encapsulation multilink-frame-relay-uni-nni;   unit 0 {     family mlfr-uni-nni {       bundle rlsq0:0;     }   } } ds-5/2/0:2:1:2 {   encapsulation multilink-frame-relay-uni-nni;   unit 0 {     family mlfr-uni-nni {       bundle rlsq0:0;     }   } } </pre>

## Verification

Confirm that the configuration is working properly.

- [Verifying the MLPPP Bundle on page 1439](#)
- [Verifying the MLFR FRF.15 Configuration on page 1439](#)
- [Verifying the MLFR FRF.16 Configuration on page 1439](#)

---

### Verifying the MLPPP Bundle

<b>Purpose</b>	Verify that the constituent links are added to the bundle correctly.
<b>Action</b>	From operational mode, enter the <b>show interfaces lsq-fpc/pic/port</b> command.
<b>Meaning</b>	The output displays the constituent links that are added to the bundle. For more information about the <b>show interfaces lsq-fpc/pic/port</b> operational command, see the <a href="#">CLI Explorer</a> .

---

### Verifying the MLFR FRF.15 Configuration

<b>Purpose</b>	Verify the MLFR FRF.15 configuration.
<b>Action</b>	From operational mode, enter the <b>show interfaces lsq-fpc/pic/port</b> command.
<b>Meaning</b>	The output displays the standard status information about the specified link services IQ interface. For more information about the <b>show interfaces lsq-fpc/pic/port</b> operational command, see the <a href="#">CLI Explorer</a> .

---

### Verifying the MLFR FRF.16 Configuration

<b>Purpose</b>	Verify the MLFR FRF.16 configuration.
<b>Action</b>	From operational mode, enter the <b>show interfaces lsq-fpc/pic/port</b> command.
<b>Meaning</b>	The output displays the standard status information about the specified link services IQ interface. For more information about the <b>show interfaces lsq-fpc/pic/port</b> operational command, see the <a href="#">CLI Explorer</a> .

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Link and Multilink Services Overview on page 1371</a></li><li>• <a href="#">Multilink Interfaces on Channelized MICs Overview on page 1379</a></li><li>• <a href="#">Example: Configuring an MLPPP Bundle on page 1420</a></li><li>• <a href="#">Example: Configuring Multilink Frame Relay FRF.15 on page 1424</a></li><li>• <a href="#">Example: Configuring Multilink Frame Relay FRF.16 on page 1427</a></li></ul>
------------------------------	--



# Summary of Multilink and Link Services Configuration Statements

The following sections explain each of the multilink and link services statements. The statements are organized alphabetically.

- [acknowledge-retries on page 1442](#)
- [acknowledge-timer on page 1443](#)
- [action-red-differential-delay on page 1443](#)
- [address \(Interfaces\) on page 1444](#)
- [bundle on page 1444](#)
- [destination \(Interfaces\) on page 1445](#)
- [disable-mlppp-inner-ppp-pfc on page 1446](#)
- [dlci on page 1446](#)
- [drop-timeout on page 1447](#)
- [family on page 1450](#)
- [fragment-threshold on page 1451](#)
- [hello-timer on page 1451](#)
- [interfaces on page 1452](#)
- [interleave-fragments on page 1452](#)
- [lmi-type on page 1453](#)
- [minimum-links on page 1453](#)
- [mlfr-uni-nni-bundle-options on page 1454](#)
- [mrru on page 1455](#)
- [mtu on page 1456](#)
- [multicast-dlci on page 1456](#)
- [n391 on page 1457](#)
- [n392 on page 1458](#)
- [n393 on page 1459](#)
- [red-differential-delay on page 1459](#)

- [short-sequence on page 1460](#)
- [t391 on page 1460](#)
- [t392 on page 1461](#)
- [unit \(Interfaces\) on page 1462](#)
- [yellow-differential-delay on page 1463](#)

---

## acknowledge-retries

---

<b>Syntax</b>	<code>acknowledge-retries <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, configure the number of retransmission attempts to be made for consecutive hello or remove link messages following the expiration of the acknowledgment timer.
<b>Options</b>	<b><i>number</i></b> —Number of retransmission attempts to be made following the expiration of the acknowledgment timer. <b>Range:</b> 1 through 5 <b>Default:</b> 2
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">action-red-differential-delay on page 1443</a>, <a href="#">hello-timer on page 1451</a></li><li>• <a href="#">Configuring Acknowledgment Timers on Link Services Physical Interfaces on page 1399</a></li></ul>

## acknowledge-timer

<b>Syntax</b>	<code>acknowledge-timer <i>milliseconds</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, configure the maximum time, in milliseconds, to wait for an add link acknowledgment, hello acknowledgment, or remove link acknowledgment message.
<b>Options</b>	<p><b><i>milliseconds</i></b>—Time to wait for an add link acknowledgment, hello acknowledgment, or remove link acknowledgment message.</p> <p><b>Range:</b> 1 through 10 milliseconds</p> <p><b>Default:</b> 4 milliseconds</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">address (Interfaces) on page 1444</a></li> <li>• <a href="#">hello-timer on page 1451</a></li> <li>• <a href="#">Configuring Acknowledgment Timers on Link Services Physical Interfaces on page 1399</a></li> </ul>

## action-red-differential-delay

<b>Syntax</b>	<code>action-red-differential-delay (disable-tx   remove-link);</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, configure the action to be taken when the differential delay exceeds the red limit.
<b>Options</b>	<p><b><i>disable-tx</i></b>—Disable transmission on the bundle link.</p> <p><b><i>remove-link</i></b>—Remove the bundle link from service.</p> <p><b>Default:</b> <i>remove-link</i></p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">yellow-differential-delay on page 1463</a></li> <li>• <a href="#">Configuring Differential Delay Alarms on Link Services Physical Interfaces with MLFR FRF.16 on page 1399</a></li> </ul>

## address (Interfaces)

---

<b>Syntax</b>	<code>address address {     destination address; }</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the interface address.
<b>Options</b>	<b>address</b> —Address of the interface.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li><li>• <a href="#">Configuring the Links in a Multilink or Link Services Bundle on page 1383</a></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## bundle

---

<b>Syntax</b>	<code>bundle (ml-<i>fpc/pic/port</i>   ls-<i>fpc/pic/port</i>);</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family mlfr-end-to-end], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family mlfr-uni-nni]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Associate the multilink interface with the logical interface it is joining.
<b>Options</b>	<b>ml-<i>fpc/pic/port</i></b> —Name of the multilink interface you are linking.  <b>ls-<i>fpc/pic/port</i></b> —Name of the link services interface you are linking.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Links in a Multilink or Link Services Bundle on page 1383</a></li></ul>

## destination (Interfaces)

<b>Syntax</b>	<code>destination address;</code>
<b>Hierarchy Level</b>	<pre>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel] [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet address <i>address</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel] [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet address <i>address</i>]</pre>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For CoS on ATM interfaces, specify the remote address of the connection.</p> <p>For point-to-point interfaces only, specify the address of the interface at the remote end of the connection.</p> <p>For tunnel and encryption interfaces, specify the remote address of the tunnel.</p>
<b>Options</b>	<b>address</b> —Address of the remote side of the connection.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Linear RED Profiles on ATM Interfaces</a></li> <li>• <a href="#">Multilink and Link Services Logical Interface Configuration Overview on page 1385</a></li> <li>• <a href="#">Configuring Encryption Interfaces on page 1101</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> <li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li> <li>• <a href="#">Configuring Unicast Tunnels on page 1567</a></li> </ul>

## disable-mlppp-inner-ppp-pfc

---

<b>Syntax</b>	<code>disable-mlppp-inner-ppp-pfc;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	For MLPPP interfaces only, disable compression of the inner PPP header in the MLPPP payload. By default, compression is enabled.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces on page 1387</a></li></ul>

## dlci

---

<b>Syntax</b>	<code>dlci <i>dlci-identifier</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For Frame Relay and Multilink Frame Relay user-to-network interface (UNI) network-to-network interface (NNI) encapsulation only, and for link services and point-to-point interfaces only, configure the data-link connection identifier (DLCI) for a permanent virtual circuit (PVC) or a switched virtual circuit (SVC).  To configure a DLCI for a point-to-multipoint interface, use the <b>multipoint-destination</b> statement to specify the DLCI.
<b>Options</b>	<b><i>dlci-identifier</i></b> —Data-link connection identifier. <b>Range:</b> 16 through 1022
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring DLCIs on Link Services Logical Interfaces on page 1393</a></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## drop-timeout

<b>Syntax</b>	<code>drop-timeout <i>milliseconds</i>;</code>
<b>Hierarchy Level</b>	<p>[edit interfaces <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a>],</p> <p>[edit interfaces (<i>ls-fpc/pic/port</i>   <i>ml-fpc/pic/port</i>) <a href="#">unit</a> <i>logical-unit-number</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces (<i>ls-fpc/pic/port</i>   <i>ml-fpc/pic/port</i>) <a href="#">unit</a> <i>logical-unit-number</i>]</p>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For multilink and link services interfaces only, configure the drop timeout period, in milliseconds.
<b>Options</b>	<p><b><i>milliseconds</i></b>—Drop timeout period.</p> <p><b>Range:</b> 1 through 2000 milliseconds</p> <p><b>Default:</b> 500 ms for bundles greater than or equal to the T1 bandwidth value, and 1500 ms for other bundles. Any CLI-configured value overrides these defaults. Setting a value of 0 reverts to the default.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring the Drop Timeout Period on Multilink and Link Services Logical Interfaces on page 1387</a></li> </ul>

## encapsulation

---

See the following sections:

- [encapsulation \(Logical Interface\) on page 1448](#)
- [encapsulation \(Physical Interface\) on page 1449](#)

### encapsulation (Logical Interface)

<b>Syntax</b>	<code>encapsulation (atm-mlppp-llc   multilink-frame-relay-end-to-end   multilink-ppp   ... );</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Logical link-layer encapsulation type.
<b>Options</b>	<p><b>atm-mlppp-llc</b>—For ATM 2 interfaces, use Multilink Point-to-Point Protocol (MLPPP) over ATM Adaptation Layer 5 (AAL5) logical link control (LLC) encapsulation, as described in RFC 2364, <i>PPP over AAL5</i>.</p> <p><b>multilink-frame-relay-end-to-end</b>—Use Multilink Frame Relay (MLFR) FRF.15 encapsulation. This encapsulation is used on multilink “link services interfaces and their constituent T1 or E1 interfaces”, and is supported on LSQ and redundant LSQ interfaces.</p> <p><b>multilink-ppp</b>—Use MLPPP encapsulation. This encapsulation is used only on multilink and link services interfaces and their constituent T1 or E1 interfaces.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Encapsulation for Multilink and Link Services Logical Interfaces on page 1386</a></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## encapsulation (Physical Interface)

<b>Syntax</b>	encapsulation (multilink-frame-relay-uni-nni   ... );
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ], [edit interfaces <i>rlsnumber:number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Physical link-layer encapsulation type.
<b>Default</b>	MLFR UNI NNI encapsulation (on link services interfaces).
<b>Options</b>	<b>multilink-frame-relay-uni-nni</b> —Use MLFR UNI NNI encapsulation. This encapsulation is used only on link services interfaces functioning as FRF.16 bundles and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Encapsulation for Link Services Physical Interfaces on page 1398</a></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## family

---

<b>Syntax</b>	<pre>family <i>family</i> {     address <i>address</i> {         destination <i>address</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure protocol family information for the logical interface.
<b>Options</b>	<p><i>family</i>—Protocol family:</p> <ul style="list-style-type: none"><li>• <b>ccc</b>—Circuit cross-connect protocol suite</li><li>• <b>inet</b>—IP version 4 (IPv4)</li><li>• <b>inet6</b>—IP version 6 (IPv6)</li><li>• <b>iso</b>—Open Systems Interconnection (OSI) International Organization for Standardization (ISO) protocol suite</li><li>• <b>mlfr-end-to-end</b>—Multilink Frame Relay FRF.15</li><li>• <b>mlfr-uni-nni</b>—Multilink Frame Relay FRF.16</li><li>• <b>multilink-ppp</b>—Multilink Point-to-Point Protocol</li><li>• <b>mpls</b>—MPLS</li><li>• <b>tcc</b>—Translational cross-connect protocol suite</li><li>• <b>tnp</b>—Trivial Network Protocol</li><li>• <b>vpls</b>—Virtual private LAN service</li></ul> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Link and Multilink Properties</i></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## fragment-threshold

<b>Syntax</b>	<code>fragment-threshold <i>bytes</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a> ], [edit interfaces ( <i>ls-fpc/pic/port</i>   <i>ml-fpc/pic/port</i> ) <a href="#">unit</a> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a> ], [edit logical-systems <i>logical-system-name</i> interfaces ( <i>ls-fpc/pic/port</i>   <i>ml-fpc/pic/port</i> ) <a href="#">unit</a> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For multilink and link services interfaces only, set the fragmentation threshold, in bytes.
<b>Options</b>	<b>bytes</b> —Maximum size, in bytes, for multilink packet fragments. Any nonzero value must be a multiple of 64 bytes. <b>Range:</b> 128 through 16,320 bytes <b>Default:</b> 0 bytes (no fragmentation)
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Limiting Packet Payload Size on Multilink and Link Services Logical Interfaces on page 1389</a></li> <li>• <a href="#">Example: Configuring a Multilink Interface with MLPPP on page 1407</a></li> </ul>

## hello-timer

<b>Syntax</b>	<code>hello-timer <i>milliseconds</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, configure the rate at which hello messages are sent. A hello message is transmitted after a period defined in milliseconds has elapsed.
<b>Options</b>	<b>milliseconds</b> —The rate at which hello messages are sent. <b>Range:</b> 1 through 180 milliseconds <b>Default:</b> 10 milliseconds
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Acknowledgment Timers on Link Services Physical Interfaces on page 1399</a></li> <li>• <a href="#">address (Interfaces) on page 1444, acknowledge-timer on page 1443</a></li> </ul>

## interfaces

---

<b>Syntax</b>	interfaces { ... }
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure interfaces on the router.
<b>Default</b>	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## interleave-fragments

---

<b>Syntax</b>	interleave-fragments;
<b>Hierarchy Level</b>	[edit interfaces ls-fpc/pic/port:channel <a href="#">unit</a> logical-unit-number], [edit logical-systems logical-system-name interfaces ls-fpc/pic/port <a href="#">unit</a> logical-unit-number]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services and voice services interfaces only, interleave long packets with high-priority packets.  Allows small delay-sensitive packets, such as voice over IP (VoIP) packets, to interleave with long fragmented packets. This minimizes the latency of delay-sensitive packets.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces on page 1394</a></li></ul>

## lmi-type

<b>Syntax</b>	<code>lmi-type (ansi   itu);</code>
<b>Hierarchy Level</b>	[edit interfaces <code>ls-fpc/pic/port:channel</code> <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Set the Frame Relay Local Management Interface (LMI) type.
<b>Options</b>	<p><b>ansi</b>—Use American National Standards Institute (ANSI) T1.167 Annex D LMIs.</p> <p><b>itu</b>—Use ITU Q933 Annex A LMIs.</p> <p><b>Default:</b> <code>itu</code></p>
<b>Required Privilege Level</b>	<p><b>interface</b>—To view this statement in the configuration.</p> <p><b>interface-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring Keepalives on Link Services Physical Interfaces on page 1400</a></li> </ul>

## minimum-links

<b>Syntax</b>	<code>minimum-links number;</code>
<b>Hierarchy Level</b>	<p>[edit interfaces <code>ls-fpc/pic/port:channel</code> <a href="#">mlfr-uni-nni-bundle-options</a>],</p> <p>[edit interfaces (<code>ls-fpc/pic/port</code>   <code>ml-fpc/pic/port</code>) <a href="#">unit</a> <code>logical-unit-number</code>],</p> <p>[edit logical-systems <code>logical-system-name</code> interfaces <code>ls-fpc/pic/port:channel</code> <a href="#">mlfr-uni-nni-bundle-options</a>],</p> <p>[edit logical-systems <code>logical-system-name</code> interfaces (<code>ls-fpc/pic/port</code>   <code>ml-fpc/pic/port</code>) <a href="#">unit</a> <code>logical-unit-number</code>]</p>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>For multilink or link services interfaces only, set the minimum number of links that must be up for the bundle to be labeled up. A member link is considered up when the PPP Link Control Protocol (LCP) phase transitions to open state.</p> <p>The <b>minimum-links</b> value should be identical on both ends of the bundle.</p>
<b>Options</b>	<p><b>number</b>—Number of links.</p> <p><b>Range:</b> 1 through 8</p> <p><b>Default:</b> 1</p>
<b>Required Privilege Level</b>	<p><b>interface</b>—To view this statement in the configuration.</p> <p><b>interface-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring the Minimum Number of Active Links on Multilink and Link Services Logical Interfaces on page 1390</a></li> </ul>

## mlfr-uni-nni-bundle-options

---

<b>Syntax</b>	<pre>mlfr-uni-nni-bundle-options {   acknowledge-retries <i>number</i>;   acknowledge-timer <i>milliseconds</i>;   action-red-differential-delay (disable-tx   remove-link);   cisco-interoperability send-lip-remove-link-for-link-reject;   drop-timeout <i>milliseconds</i>;   fragment-threshold <i>bytes</i>;   hello-timer <i>milliseconds</i>;   lmi-type (ansi   itu   c-lmi);   minimum-links <i>number</i>;   mrru <i>bytes</i>;   n391 <i>number</i>;   n392 <i>number</i>;   n393 <i>number</i>;   red-differential-delay <i>milliseconds</i>;   t391 <i>number</i>;   t392 <i>number</i>;   yellow-differential-delay <i>milliseconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>ls-fpc/pic/port</i> : <i>channel</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure link services interface management properties.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Encapsulation for Link Services Physical Interfaces on page 1398</a></li></ul>

## mrru

<b>Syntax</b>	<code>mrru bytes;</code>
<b>Hierarchy Level</b>	<p>[edit interfaces <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a>],</p> <p>[edit interfaces (<i>ml-fpc/pic/port</i>  <i>ls-fpc/pic/port</i>) <a href="#">unit</a> <i>logical-unit-number</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces (<i>ml-fpc/pic/port</i>  <i>ls-fpc/pic/port</i>) <a href="#">unit</a> <i>logical-unit-number</i>]</p>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For multilink or link services interfaces only, set the maximum received reconstructed unit (MRRU). The MRRU is similar to the maximum transmission unit (MTU), but is specific to multilink interfaces.
<b>Options</b>	<p><i>bytes</i>—MRRU size.</p> <p><b>Range:</b> 1500 through 4500 bytes</p> <p><b>Default:</b> 1500 bytes</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring MRRU on Multilink and Link Services Logical Interfaces on page 1391</a></li> </ul>

## mtu

---

<b>Syntax</b>	<code>mtu bytes;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ], [edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> <i>family</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> <i>family</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Maximum transmission unit (MTU) size for the media or protocol. The default MTU size depends on the device type. Not all devices allow you to set an MTU value, and some devices have restrictions on the range of allowable MTU values.
<b>Options</b>	<b>bytes</b> —MTU size. <b>Range:</b> 0 through 5012 bytes <b>Default:</b> 1500 bytes ( <b>inet</b> , <b>inet6</b> , and <b>iso</b> families), 1448 bytes ( <b>mpls</b> )
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring MRRU on Multilink and Link Services Logical Interfaces on page 1391</a></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li></ul>

## multicast-dlci

---

<b>Syntax</b>	<code>multicast-dlci <i>dlci-identifier</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For point-to-multipoint link services interfaces only, enable multicast support on the interface. You can configure multicast support on the interface if the Frame Relay switch performs multicast replication.
<b>Options</b>	<b><i>dlci-identifier</i></b> —DLCI identifier, a number from 16 through 1022 that defines the Frame Relay DLCI over which the switch expects to receive multicast packets for replication.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Multicast-Capable DLCIs for MLFR FRF.16 Bundles on page 1393</a></li></ul>

## n391

---

<b>Syntax</b>	n391 <i>number</i> ;
<b>Hierarchy Level</b>	[edit interfaces ls-fpc/pic/port:channel <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, set the Frame Relay full status polling interval.
<b>Options</b>	<i>number</i> —Polling interval. <b>Range:</b> 1 through 255 <b>Default:</b> 6
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Keepalives on Link Services Physical Interfaces on page 1400</a></li><li>• <a href="#">n392 on page 1458</a></li><li>• <a href="#">, n393 on page 1459</a></li><li>• <a href="#">t391 on page 1460</a></li><li>• <a href="#">t392 on page 1461</a></li></ul>

## n392

---

<b>Syntax</b>	<code>n392 number;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, set the Frame Relay error threshold, in number of errors.
<b>Options</b>	<i>number</i> —Error threshold. <b>Range:</b> 1 through 10 <b>Default:</b> 3
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Keepalives on Link Services Physical Interfaces on page 1400</a></li><li>• <a href="#">n391 on page 1457</a></li><li>• <a href="#">n393 on page 1459</a></li><li>• <a href="#">t391 on page 1460</a></li><li>• <a href="#">t392 on page 1461</a></li></ul>

## n393

---

<b>Syntax</b>	<code>n393 number;</code>
<b>Hierarchy Level</b>	[edit interfaces ls-fpc/pic/port:channel <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, set the Frame Relay monitored event count.
<b>Options</b>	<p><i>number</i>—Event count.</p> <p><b>Range:</b> 1 through 10</p> <p><b>Default:</b> 4</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Keepalives on Link Services Physical Interfaces on page 1400</a></li> <li>• <a href="#">n391 on page 1457</a></li> <li>• <a href="#">n392 on page 1458</a></li> <li>• <a href="#">t391 on page 1460</a></li> <li>• <a href="#">t392 on page 1461</a></li> </ul>

## red-differential-delay

---

<b>Syntax</b>	<code>red-differential-delay milliseconds;</code>
<b>Hierarchy Level</b>	[edit interfaces ls-fpc/pic/port:channel <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, configure the red differential delay among bundle links to give warning when a link has a differential delay that exceeds the configured threshold.
<b>Options</b>	<p><i>milliseconds</i>—Red differential delay threshold.</p> <p><b>Range:</b> 1 through 2000 milliseconds</p> <p><b>Default:</b> 120 milliseconds</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Differential Delay Alarms on Link Services Physical Interfaces with MLFR FRF.16 on page 1399</a></li> <li>• <a href="#">action-red-differential-delay on page 1443,</a></li> <li>• <a href="#">yellow-differential-delay on page 1463</a></li> </ul>

## short-sequence

---

<b>Syntax</b>	short-sequence;
<b>Hierarchy Level</b>	[edit interfaces (ls-fpc/pic/port   ml-fpc/pic/port) <b>unit</b> logical-unit-number], [edit logical-systems logical-system-name interfaces (ls-fpc/pic/port   ml-fpc/pic/port) <b>unit</b> logical-unit-number]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For multilink interfaces only, set the length of the packet sequence identification number to 12 bits.
<b>Default</b>	If not included in the configuration, the length is set to 24 bits.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Sequence Header Format on Multilink and Link Services Logical Interfaces on page 1392</a></li></ul>

## t391

---

<b>Syntax</b>	t391 <i>number</i> ;
<b>Hierarchy Level</b>	[edit interfaces ls-fpc/pic/port:channel <b>mlfr-uni-nni-bundle-options</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, set the Frame Relay link integrity polling interval.
<b>Options</b>	<i>number</i> —Link integrity polling interval. <b>Range:</b> 5 through 30 seconds <b>Default:</b> 10 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Keepalives on Link Services Physical Interfaces on page 1400</a></li><li>• <a href="#">n391 on page 1457</a></li><li>• <a href="#">n392 on page 1458</a></li><li>• <a href="#">t392 on page 1461</a></li><li>• <a href="#">n393 on page 1459</a></li></ul>

## t392

---

<b>Syntax</b>	t392 <i>number</i> ;
<b>Hierarchy Level</b>	[edit interfaces ls-fpc/pic/port:channel <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, set the Frame Relay polling verification interval.
<b>Options</b>	<i>number</i> —Polling verification interval. <b>Range:</b> 5 through 30 seconds <b>Default:</b> 15 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Keepalives on Link Services Physical Interfaces on page 1400</a></li><li>• <a href="#">n391 on page 1457</a></li><li>• <a href="#">n392 on page 1458</a></li><li>• <a href="#">n393 on page 1459</a></li><li>• <a href="#">t391 on page 1460</a></li></ul>

## unit (Interfaces)

---

<b>Syntax</b>	<pre>unit logical-unit-number {   disable-mlppp-inner-ppp-pfc;   dlci dlci-identifier;   drop-timeout milliseconds;   encapsulation type;   fragment-threshold bytes;   interleave-fragments;   minimum-links number;   mrru bytes;   multicast-dlci dlci-identifier;   short-sequence;   family family {     address address {       destination address;     }     bundle (ml-fpc/pic/port   ls-fpc/pic/port);   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> interface-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
<b>Options</b>	<p><i>logical-unit-number</i>—Number of the logical unit.</p> <p><b>Range:</b> 0 through 16,384</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Link and Multilink Properties</i></li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li></ul>

## yellow-differential-delay

---

<b>Syntax</b>	<code>yellow-differential-delay <i>milliseconds</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>ls-fpc/pic/port:channel</i> <a href="#">mlfr-uni-nni-bundle-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For link services interfaces only, configure the yellow differential delay among bundle links to give warning when a link has a differential delay that exceeds the configured threshold.
<b>Options</b>	<p><i>milliseconds</i>—Yellow differential delay threshold.</p> <p><b>Range:</b> 1 through 2000 milliseconds</p> <p><b>Default:</b> 72 milliseconds</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Differential Delay Alarms on Link Services Physical Interfaces with MLFR FRF.16 on page 1399</a></li><li>• <a href="#">action-red-differential-delay on page 1443</a></li><li>• <a href="#">red-differential-delay on page 1459</a></li></ul>



## PART 7

# Real-Time Performance Monitoring Services

- [Real-Time Performance Monitoring Services Overview on page 1467](#)
- [Real-Time Performance Monitoring Configuration Guidelines on page 1471](#)
- [Summary of Real-Time Performance Monitoring Configuration Statements on page 1521](#)



# Real-Time Performance Monitoring Services Overview

## Real-Time Performance Monitoring Services Overview

---

Real-Time Performance Monitoring (RPM) enables you to configure active probes to track and monitor traffic. Probes collect packets per destination and per application, including PING Internet Control Message Protocol (ICMP) packets, User Datagram Protocol and Transmission Control Protocol (UDP/TCP) packets with user-configured ports, user-configured Differentiated Services code point (DSCP) type-of-service (ToS) packets, and Hypertext Transfer Protocol (HTTP) packets. RPM provides Management Information Base (MIB) support with extensions for RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*.

You can also configure RPM services to determine automatically whether a path exists between a host router and its configured BGP neighbors. You can view the results of the discovery using an SNMP client. Results are stored in **pingResultsTable**, **jnxPingResultsTable**, **jnxPingProbeHistoryTable**, and **pingProbeHistoryTable**.

Probe configuration and probe results are supported by the command-line interface (CLI) and SNMP.

The following probe types are supported with DSCP marking:

- ICMP echo
- ICMP timestamp
- HTTP get (not available for BGP RPM services)
- UDP echo
- TCP connection
- UDP timestamp

With probes, you can monitor the following:

- Minimum round-trip time
- Maximum round-trip time
- Average round-trip time

- Standard deviation of the round-trip time
- Jitter of the round-trip time—The difference between the minimum and maximum round-trip time

One-way measurements for ICMP timestamp probes include the following:

- Minimum, maximum, standard deviation, and jitter measurements for egress and ingress times
- Number of probes sent
- Number of probe responses received
- Percentage of lost probes



**NOTE:** Timestamping is not supported on PTX Series Packet Transport Routers.

---

You can configure the following RPM thresholds:

- Round-trip time
- Ingress/egress delay
- Standard deviation
- Jitter
- Successive lost probes
- Total lost probes (per test)

Support is also implemented for user-configured CoS classifiers and for prioritization of RPM packets over regular data packets received on an input interface.

**Related  
Documentation**

- [Configuring BGP Neighbor Discovery Through RPM on page 1473](#)
- [\[edit services rpm\] Hierarchy Level on page 1471](#)
- [Examples: Configuring BGP Neighbor Discovery Through RPM on page 1515](#)

---

## RFC 2544-Based Benchmarking Tests Overview

---

RFC 2544 defines a series of tests that can be used to describe the performance characteristics of a network-interconnecting device, such as a router, and outlines specific formats to report the results of the tests. These tests can be used to benchmark interconnected network devices and devise a guideline or a measurement pattern to analyze the health and efficiency of the network devices. Because of the ability of these tests to measure throughput, bursty frames, frame loss, and latency, this mechanism is also used to diagnose Ethernet-based networks. These tests are the standard benchmarking tests for Ethernet networks and are known as RFC 2544-based benchmarking tests. The test methodology enables you to define various parameters

such as different frame sizes to be examined (64, 128, 256, 512, 1024, 1280 and 1518 bytes), the test time for each test iteration, and the frame format (IP or UDP).

In Junos OS Release 13.3, MX104 routers support only the reflector function and the corresponding benchmarking tests. These tests display only the reflected bytes and packets on the routers.

RFC 2544-based benchmarking test is performed by transmitting test packets from a device that functions as the generator or the initiator. The initiator is also called the originator. These packets are sent to a device that functions as the reflector, which receives and returns the packets back to the initiator.

The RFC 2544 methodology assesses different parameters that are defined in service-level agreements (SLAs). By measuring the performance availability, transmission delay, link bursts, and service integrity, a carrier provider can certify that the working parameters of the deployed Ethernet circuit comply with the SLA and other defined policies.

[Table 43 on page 1469](#) describes the different network topologies in which the benchmarking test is supported:

**Table 43: Supported Network Topologies for RFC 2544 Benchmarking Tests**

Type of Network	Traffic Direction	Supported Packet Types	Whether the Benchmarking Test Is Supported
Ethernet pseudowire	Ingress and Egress	All EtherTypes for Ingress and MPLS encapsulated packets for Egress	Supported
Layer 3 IPv4	Egress	IPv4 in Layer 3 and any protocol in Layer 2	Supported

**Related Documentation**

- [Configuring an RFC 2544-Based Benchmarking Test on page 1489](#)



## CHAPTER 61

# Real-Time Performance Monitoring Configuration Guidelines

This chapter includes the following sections:

- [\[edit services rpm\] Hierarchy Level on page 1471](#)
- [Configuring BGP Neighbor Discovery Through RPM on page 1473](#)
- [Configuring RPM Probes on page 1475](#)
- [Configuring RPM Receiver Servers on page 1480](#)
- [Limiting the Number of Concurrent RPM Probes on page 1481](#)
- [Configuring RPM Timestamping on page 1481](#)
- [Configuring TWAMP on page 1484](#)
- [Enabling RPM for the Junos OS extension-provider package on page 1486](#)
- [Tracing RPM Operations on page 1487](#)
- [Configuring an RFC 2544-Based Benchmarking Test on page 1489](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for Layer 3 IPv4 Services on page 1492](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for UNI Direction of Ethernet Pseudowires on page 1500](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for NNI Direction of Ethernet Pseudowires on page 1507](#)
- [Examples: Configuring BGP Neighbor Discovery Through RPM on page 1515](#)
- [Examples: Configuring Real-Time Performance Monitoring on page 1516](#)

### [\[edit services rpm\] Hierarchy Level](#)

---

To configure Real-Time Performance Monitoring (RPM) services, include the **rpm** statement at the **[edit services]** hierarchy level:

```
[edit services]
rpm {
  bgp {
    data-fill data;
    data-size size;
```

```

destination-port port;
history-size size;
logical-system logical-system-name [routing-instances routing-instance-name];
moving-average-size number;
probe-count count;
probe-interval seconds;
probe-type type;
routing-instances instance-name;
test-interval interval;
}
probe owner {
  test test-name {
    data-fill data;
    data-size size;
    destination-interface interface-name;
    destination-port port;
    dscp-code-point dscp-bits;
    hardware-timestamp;
    history-size size;
    moving-average-size number;
    one-way-hardware-timestamp;
    probe-count count;
    probe-interval seconds;
    probe-type type;
    routing-instance instance-name;
    source-address address;
    target (url url | address address);
    test-interval interval;
    thresholds thresholds;
    traps traps;
  }
}
probe-server {
  tcp {
    destination-interface interface-name;
    port number;
  }
  udp {
    destination-interface interface-name;
    port number;
  }
}
probe-limit limit;
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
}
twamp {
  server {
    authentication-mode (authenticated | encrypted | none);
    client-list list-name {
      [ address address ];
    }
    inactivity-timeout seconds;
    maximum-connections-duration hours;
  }
}

```

```

        maximum-connections count;
        maximum-connections-per-client count;
        maximum-sessions count;
        maximum-sessions-per-connection count;
        port number;
        server-inactivity-timeout minutes;
    }
}
rfc2544-benchmarking {
    tests{
        test-name (RFC 2544 Benchmarking) test-name {
            test-interface interface-name;
            mode reflect;
            family (inet | ccc);
            destination-ipv4-address address;
            destination-udp-port port-number;
            source-ipv4-address address;
            source-udp-port port-number;
            direction (egress | ingress);
        }
    }
}

```



NOTE: RPM does not require an Adaptive Services (AS) or Multiservices PIC or Multiservices Dense Port Concentrator (DPC) unless you are configuring RPM timestamping as described in “[Configuring RPM Timestamping](#)” on [page 1481](#).

#### Related Documentation

- [Configuring BGP Neighbor Discovery Through RPM on page 1473](#)
- [Configuring RPM Probes on page 1475](#)
- [Configuring RPM Receiver Servers on page 1480](#)
- [Limiting the Number of Concurrent RPM Probes on page 1481](#)
- [Configuring RPM Timestamping on page 1481](#)
- [Configuring TWAMP on page 1484](#)
- [Enabling RPM for the Junos OS extension-provider package on page 1486](#)
- [Tracing RPM Operations on page 1487](#)

## Configuring BGP Neighbor Discovery Through RPM

BGP neighbors can be configured at the following hierarchy levels:

- **[edit protocols bgp group *group-name*]**—Default logical system and default routing instance.
- **[edit routing-instances *instance-name* protocols bgp group *group-name*]**—Default logical system with a specified routing instance.

- **[edit logical-systems *logical-system-name* protocols bgp group *group-name*]**—Configured logical system and default routing instance.
- **[edit logical-systems *logical-system-name* routing-instances *instance-name* protocols bgp group *group-name*]**—Configured logical system with a specified routing instance.

When you configure BGP neighbor discovery through RPM, if you do not specify a logical system, the RPM probe applies to configured BGP neighbors for all logical systems. If you do not specify a routing instance, the RPM probe applies to configured BGP neighbors in all routing instances. You can explicitly configure RPM probes to apply only to the default logical system, the default routing instance, or to a particular logical system or routing instance.

To configure BGP neighbor discovery through RPM, configure the probe properties at the **[edit services rpm bgp]** hierarchy:

```
data-fill data;  
data-size size;  
destination-port port;  
history-size size;  
logical-system logical-system-name [routing-instances routing-instance-name];  
moving-average-size number;  
probe-count count;  
probe-interval seconds;  
probe-type type;  
routing-instances instance-name;  
test-interval interval;
```

- To specify the contents of the data portion of Internet Control Message Protocol (ICMP) probes, include the **data-fill** statement at the **[edit services rpm bgp]** hierarchy level. The value can be a hexadecimal value.
- To specify the size of the data portion of ICMP probes, include the **data-size** statement at the **[edit services rpm bgp]** hierarchy level. The size can be from **0** through **65400** and the default size is **0**.
- To specify the User Datagram Protocol (UDP) port or Transmission Control Protocol (TCP) port to which the probe is sent, include the **destination-port** statement at the **[edit services rpm bgp]** hierarchy level. The **destination-port** statement is used only for the UDP and TCP probe types. The value can be **7** or from **49160** through **65535**.
- To specify the number of stored history entries, include the **history-size** statement at the **[edit services rpm bgp]** hierarchy level. Specify a value from **0** to **512**. The default is **50**.
- To specify the logical system used by ICMP probes, include the **logical-system *logical-system-name*** statement at the **[edit services rpm bgp]** hierarchy level. If you do not specify a logical system, the RPM probe applies to configured BGP neighbors for all logical systems. To apply the probe to only the default logical system, you must set the value of **logical-system-name** to **null**.
- To specify a number of samples for making statistical calculations, include the **moving-average-size** statement at the **[edit services rpm bgp]** hierarchy level. Specify a value from **0** through **255**.

- To specify the number of probes within a test, include the **probe-count** statement at the **[edit services rpm bgp]** hierarchy level. Specify a value from 1 through 15.
- To specify the time to wait between sending packets, include the **probe-interval** statement at the **[edit services rpm bgp]** hierarchy level. Specify a value from 1 through 255 seconds.
- To specify the packet and protocol contents of the probe, include the **probe-type** statement at the **[edit services rpm bgp]** hierarchy level. The following probe types are supported:
  - **icmp-ping**—Sends ICMP echo requests to a target address.
  - **icmp-ping-timestamp**—Sends ICMP timestamp requests to a target address.
  - **tcp-ping**—Sends TCP packets to a target.
  - **udp-ping**—Sends UDP packets to a target.
  - **udp-ping-timestamp**—Sends UDP timestamp requests to a target address.



**NOTE:** Some probe types require additional parameters to be configured. For example, when you specify the **tcp-ping** or **udp-ping** option, you must configure the destination port using the **destination-port port** statement. The **udp-ping-timestamp** option requires a minimum data size of 12; any smaller data size results in a commit error. The minimum data size for TCP probe packets is 1.

- To specify the routing instance used by ICMP probes, include the **routing-instances** statement at the **[edit services rpm bgp]** hierarchy level. The default routing instance is Internet routing table **inet.0**. If you do not specify a routing instance, the RPM probe applies to configured BGP neighbors in all routing instances. To apply the RPM probe to only the default routing instance, you must explicitly set the value of **instance-name** to **default**.
- To specify the time to wait between tests, include the **test-interval** statement at the **[edit services bgp probe]** hierarchy level. Specify a value from 0 through 86400 seconds.

#### Related Documentation

- [Real-Time Performance Monitoring Services Overview on page 1467](#)
- [\[edit services rpm\] Hierarchy Level on page 1471](#)
- [Examples: Configuring BGP Neighbor Discovery Through RPM on page 1515](#)

## Configuring RPM Probes

The owner name and test name identifiers of an RPM probe together represent a single RPM configuration instance. When you specify the test name, you also can configure the test parameters.

To configure the probe owner, test name, and test parameters, include the **probe** statement at the **[edit services rpm]** hierarchy level:

```
probe owner {  
  test test-name {  
    data-fill data;  
    data-size size;  
    destination-interface interface-name;  
    destination-port port;  
    dscp-code-point dscp-bits;  
    hardware-timestamp;  
    history-size size;  
    moving-average-size number;  
    one-way-hardware-timestamp;  
    probe-count count;  
    probe-interval seconds;  
    probe-type type;  
    routing-instance instance-name;  
    source-address address;  
    target (url url | address address);  
    test-interval interval;  
    thresholds thresholds;  
    traps traps;  
  }  
}
```

Keep the following points in mind when you configure RPM clients and RPM servers:

- You cannot configure an RPM client that is PIC-based and an RPM server that is based on either the Packet Forwarding Engine or Routing Engine to receive the RPM probes.
- You cannot configure an RPM client that is Packet Forwarding Engine-based and an RPM server that receives the RPM probes to be on the PIC or Routing Engine.
- The RPM client and RPM server must be located on the same type of module. For example, if the RPM client is PIC-based, the RPM server must also be PIC-based, and if the RPM server is Packet Forwarding Engine-based, the RPM client must also be Packet Forwarding Engine-based.
- To specify a probe owner, include the **probe** statement at the **[edit services rpm]** hierarchy level. The probe owner identifier can be up to 32 characters in length.
- To specify a test name, include the **test** statement at the **[edit services rpm probe owner]** hierarchy level. The test name identifier can be up to 32 characters in length. A test represents the range of probes over which the standard deviation, average, and jitter are calculated.
- To specify the contents of the data portion of Internet Control Message Protocol (ICMP) probes, include the **data-fill** statement at the **[edit services rpm probe owner]** hierarchy level. The value can be a hexadecimal value. The **data-fill** statement is not valid with the **http-get** or **http-metadata-get** probe types.
- To specify the size of the data portion of ICMP probes, include the **data-size** statement at the **[edit services rpm probe owner]** hierarchy level. The size can be from **0** through **65400** and the default size is **0**. The **data-size** statement is not valid with the **http-get** or **http-metadata-get** probe types.



**NOTE:** If you configure the hardware timestamp feature (see [“Configuring RPM Timestamping” on page 1481](#)):

- The **data-size** default value is 32 bytes and 32 is the minimum value for explicit configuration. The UDP timestamp probe type is an exception; it requires a minimum data size of 44 bytes.
- The **data-size** must be at least 100 bytes smaller than the default MTU of the interface of the RPM client interface.

- On M Series and T Series routers, you configure the **destination-interface** statement to enable hardware timestamping of RPM probe packets. You specify an **sp-** interface to have the AS or Multiservices PIC add the hardware timestamps; for more information, see [“Configuring RPM Timestamping” on page 1481](#). You can also include the **one-way-hardware-timestamp** statement to enable one-way delay and jitter measurements.
- To specify the User Datagram Protocol (UDP) port or Transmission Control Protocol (TCP) port to which the probe is sent, include the **destination-port** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. The **destination-port** statement is used only for the UDP and TCP probe types. The value can be 7 or from 49160 through 65535.

When you configure either **probe-type udp-ping** or **probe-type udp-ping-timestamp** along with hardware timestamping, the value for the **destination-port** can be only 7. A constraint check prevents you from configuring any other value for the destination port in this case. This constraint does not apply when you are using one-way hardware timestamping.

- To specify the value of the Differentiated Services (DiffServ) field within the IP header, include the **dscp-code-point** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. The DiffServ code point (DSCP) bits value can be set to a valid 6-bit pattern; for example, 001111. It also can be set using an alias configured at the **[edit class-of-service code-point-aliases dscp]** hierarchy level. The default is 000000.
- To specify the number of stored history entries, include the **history-size** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. Specify a value from 0 to 512. The default is 50.
- To specify a number of samples for making statistical calculations, include the **moving-average-size** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. Specify a value from 0 through 255.
- To specify the number of probes within a test, include the **probe-count** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. Specify a value from 1 through 15.
- To specify the time to wait between sending packets, include the **probe-interval** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. Specify a value from 1 through 255 seconds.

- To specify the packet and protocol contents of the probe, include the **probe-type** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. The following probe types are supported:
  - **http-get**—Sends a Hypertext Transfer Protocol (HTTP) get request to a target URL.
  - **http-metadata-get**—Sends an HTTP get request for metadata to a target URL.
  - **icmp-ping**—Sends ICMP echo requests to a target address.
  - **icmp-ping-timestamp**—Sends ICMP timestamp requests to a target address.
  - **tcp-ping**—Sends TCP packets to a target.
  - **udp-ping**—Sends UDP packets to a target.
  - **udp-ping-timestamp**—Sends UDP timestamp requests to a target address.

The following probe types support hardware timestamping of probe packets: **icmp-ping**, **icmp-ping-timestamp**, **udp-ping**, **udp-ping-timestamp**.



**NOTE:** Some probe types require additional parameters to be configured. For example, when you specify the **tcp-ping** or **udp-ping** option, you must configure the destination port using the **destination-port** statement. The **udp-ping-timestamp** option requires a minimum data size of 12; any smaller data size results in a commit error. The minimum data size for TCP probe packets is 1.

When you configure either **probe-type udp-ping** or **probe-type udp-ping-timestamp** along with the **one-way-hardware-timestamp** command, the value for the **destination-port** can be only 7. A constraint check prevents you for configuring any other value for the destination port in this case.

- To specify the routing instance used by ICMP probes, include the **routing-instance** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. The default routing instance is Internet routing table **inet.0**.
- To specify the source IP address used for ICMP probes, include the **source-address** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. If the source IP address is not one of the router's assigned addresses, the packet will use the outgoing interface's address as its source.
- To specify the destination address used for the probes, include the **target** statement at the **[edit services rpm probe owner test test-name]** hierarchy level.
  - For HTTP probe types, specify a fully formed URL that includes **http://** in the URL address.
  - For all other probe types, specify an IP version 4 (IPv4) address for the target host.
- To specify the time to wait between tests, include the **test-interval** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. Specify a value from 0 through 86400 seconds.

- To specify thresholds used for the probes, include the **thresholds** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. A system log message is generated when the configured threshold is exceeded. Likewise, an SNMP trap (if configured) is generated when a threshold is exceeded. The following options are supported:
  - **egress-time**—Measures maximum source-to-destination time per probe.
  - **ingress-time**—Measures maximum destination-to-source time per probe.
  - **jitter-egress**—Measures maximum source-to-destination jitter per test.
  - **jitter-ingress**—Measures maximum destination-to-source jitter per test.
  - **jitter-rtt**—Measures maximum jitter per test, from 0 through 60000000 microseconds.
  - **rtt**—Measures maximum round-trip time per probe, in microseconds.
  - **std-dev-egress**—Measures maximum source-to-destination standard deviation per test.
  - **std-dev-ingress**—Measures maximum destination-to-source standard deviation per test.
  - **std-dev-rtt**—Measures maximum standard deviation per test, in microseconds.
  - **successive-loss**—Measures successive probe loss count, indicating probe failure.
  - **total-loss**—Measures total probe loss count indicating test failure, from 0 through 15.
- Traps are sent if the configured threshold is met or exceeded. To set the trap bit to generate traps, include the **traps** statement at the **[edit services rpm probe owner test test-name]** hierarchy level. The following options are supported:
  - **egress-jitter-exceeded**—Generates traps when the jitter in egress time threshold is met or exceeded.
  - **egress-std-dev-exceeded**—Generates traps when the egress time standard deviation threshold is met or exceeded.
  - **egress-time-exceeded**—Generates traps when the maximum egress time threshold is met or exceeded.
  - **ingress-jitter-exceeded**—Generates traps when the jitter in ingress time threshold is met or exceeded.
  - **ingress-std-dev-exceeded**—Generates traps when the ingress time standard deviation threshold is met or exceeded.
  - **ingress-time-exceeded**—Generates traps when the maximum ingress time threshold is met or exceeded.
  - **jitter-exceeded**—Generates traps when the jitter in round-trip time threshold is met or exceeded.
  - **probe-failure**—Generates traps for successive probe loss thresholds crossed.

- **rtt-exceeded**—Generates traps when the maximum round-trip time threshold is met or exceeded.
- **std-dev-exceeded**—Generates traps when the round-trip time standard deviation threshold is met or exceeded.
- **test-completion**—Generates traps when a test is completed.
- **test-failure**—Generates traps when the total probe loss threshold is met or exceeded.

**Related  
Documentation**

- [Real-Time Performance Monitoring Services Overview on page 1467](#)
- [Examples: Configuring Real-Time Performance Monitoring on page 1516](#)
- [\[edit services rpm\] Hierarchy Level on page 1471](#)

---

## Configuring RPM Receiver Servers

The RPM TCP and UDP probes are proprietary to Juniper Networks and require a receiver to receive the probes. To configure a server to receive the probes, include the **probe-server** statement at the **[edit services rpm]** hierarchy level:

```
[edit services rpm]
probe-server {
  tcp {
    destination-interface interface-name;
    port number;
  }
  udp {
    port number;
  }
}
```

The port number specified for the UDP and TCP server can be 7 or from 49160 through 65535.



**NOTE:** The **destination-interface** statement is not supported on PTX Series Packet Transport Routers.

---

When you configure either **probe-type udp-ping** or **probe-type udp-ping-timestamp** along with the **one-way-hardware-timestamp** command, the value for the **destination-port** can be only 7. A constraint check prevents you for configuring any other value for the destination port in this case.

**Related  
Documentation**

- [Real-Time Performance Monitoring Services Overview on page 1467](#)
- [\[edit services rpm\] Hierarchy Level on page 1471](#)
- [Examples: Configuring Real-Time Performance Monitoring on page 1516](#)

## Limiting the Number of Concurrent RPM Probes

To configure the maximum number of concurrent probes allowed, include the **probe-limit** statement at the **[edit services rpm]** hierarchy level:

```
probe-limit limit;
```

Specify a limit from 1 through **500**. The default maximum number is 100.

### Related Documentation

- [Real-Time Performance Monitoring Services Overview on page 1467](#)
- [\[edit services rpm\] Hierarchy Level on page 1471](#)
- [Examples: Configuring Real-Time Performance Monitoring on page 1516](#)

## Configuring RPM Timestamping

To account for latency in the communication of probe messages, you can enable timestamping of the probe packets. You can timestamp the following RPM probe types: **icmp-ping**, **icmp-ping-timestamp**, **udp-ping**, and **udp-ping-timestamp**.

On M Series and T Series routers with an Adaptive Services (AS) or Multiservices PIC, and MX Series routers with a Multiservices DPC, and on EX Series switches, you can enable hardware timestamping of RPM probe messages. The timestamp is applied on both the RPM client router (the router or switch that originates the RPM probes) and the RPM probe server and applies only to IPv4 traffic. It is supported on the following:

- Layer 2 services package on all Multiservices PICs and DPCs.
- Layer 3 service package on AS and Multiservices PICs and Multiservices DPCs.
- Extension-provider services package on M Series, MX Series, and T Series services PICs that support the Extension-Provider packages (In Junos OS releases earlier than 12.3, the extension-provider packages were variously referred to as Junos Services Framework (JSF), MP-SDK, and eJunos.)
- Layer 2, Layer 3, SDK Services, and PFE RPM timestamping interoperate with each other. Here, the RPM client can be on the Layer 3 **sp-** interface and the RPM server can be on an SDK Services package.



**NOTE:** Hardware timestamping is not supported on PTX Series Packet Transport Routers.

Two-way timestamping is available on **sp-** and **ms-** interfaces. To configure two-way timestamping on M Series and T Series routers, include the **destination-interface** statement at the **[edit services rpm probe probe-owner test test-name]** hierarchy level:

```
destination-interface sp-fpc/pic/port.logical-unit
destination-interface ms-fpc/pic/port.logical-unit
```

Specify the RPM client router and the RPM server router on the adaptive services logical interface or the multiservices interface by including the **rpm** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level:

```
rpm (client | server);
```

The logical interface must be dedicated to the RPM task. It requires configuration of the **family inet** statement and a **/32** address, as shown in the example. This configuration is also needed for other services such as NAT and stateful firewall. You cannot configure RPM service on **unit 0** because RPM requires a dedicated logical interface; the same unit cannot support both RPM and other services. Because active flow monitoring requires **unit 0**, but RPM can function on any logical interface, a constraint check prevents you from committing an RPM configuration there.



**NOTE:** If you configure RPM timestamping on an ASP PIC, you cannot configure the **source-address** statement at the **[edit services rpm probe *probe-name* test *test-name*]** hierarchy level.

On MX Series routers, on M-320 routers using the Enhanced Queuing MPC, and on EX Series switches, you include the **hardware-timestamp** statement at the **[edit services rpm probe *probe-name* test *test-name*]** hierarchy level to specify that the probes are to be timestamped in the Packet Forwarding Engine host processor:

```
hardware-timestamp;
```

On the client side, these probes are timestamped in the Packet Forwarding Engine host processor on the egress DPC on the MX or M-320 Series router or EX Series switch originating the RPM probes (RPM client). On the responder side (RPM server), the RPM probes to be timestamped are handled by the Packet Forwarding Engine host processor, which generates the response instead of the RPM process. The RPM probes are timestamped only on the router that originates them (RPM client). As a result, only round-trip time is measured for these probes.

When using the **hardware-timestamp**, the **data-size** value for the probe must be at least 100 bytes smaller than the default MTU of the interface of the RPM client interface (see “Configuring RPM Probes” on page 1475).



**NOTE:** The Packet Forwarding Engine-based RPM feature does not support any stateful firewall configurations. If you need to combine RPM timestamping with a stateful firewall, you should use the interface-based RPM timestamping service described earlier in this section. Multiservices DPCs support stateful firewall processing as well as RPM timestamping.

To configure one-way timestamping, you must also include the **one-way-hardware-timestamp** statement at the **[edit services rpm probe *probe-owner* test *test-name*]** hierarchy level:

```
one-way-hardware-timestamp;
```



**NOTE:** If you configure RPM probes for a services interface (sp-), you need to announce local routes in a specific way for the following routing protocols:

- For OSPF, you can announce the local route by including the services interface in the OSPF area. To configure this setting, include the interface `sp-fpc/pic/port` statement at the `[edit protocols ospf area area-number]` hierarchy level.
- For BGP and IS-IS, you must export interface routes and create a policy that accepts the services interface local route. To export interface routes, include the `point-to-point` and `lan` statements at the `[edit routing-options interface-routes family inet export]` hierarchy level. To configure an export policy that accepts the services interface local route, include the `protocol local`, `rib inet.0`, and `route-filter sp-interface-ip-address/32` exact statements at the `[edit policy-options policy-statement policy-name term term-name from]` hierarchy level and the `accept` action at the `[edit policy-options policy-statement policy-name term term-name then]` hierarchy level. For the export policy to take effect, apply the policy to BGP or IS-IS with the `export policy-name` statement at the `[edit protocols protocol-name]` hierarchy level.

For more information about these configurations, see the *Routing Policy Feature Guide for Routing Devices* or the *Junos OS Routing Protocols Library for Routing Devices*.

Routing the probe packets through the adaptive services or Multiservices PIC also enables you to filter the probe packets to particular queues. The following example shows the RPM configuration and the filter that specifies queuing:

```
services rpm {
  probe p1 {
    test t1 {
      probe-type icmp-ping;
      target address 10.8.4.1;
      probe-count 10;
      probe-interval 10;
      test-interval 10;
      dscp-code-points af11;
      data-size 100;
      destination-interface sp-1/2/0.0;
    }
  }
}
firewall {
  filter f1 {
    term t1 {
      from {
        dscp af11;
      }
      then {
        forwarding-class assured-forwarding;
      }
    }
  }
}
```

```
    }  
  }  
}  
interfaces sp-1/2/0 {  
  unit 2 {  
    rpm client;  
    family inet {  
      address 10.8.4.2/32;  
      filter {  
        input f1;  
      }  
    }  
  }  
}  
interfaces sp-1/2/1 {  
  unit 2 {  
    rpm server;  
    family inet {  
      address 10.8.3.2/32;  
      filter {  
        input f1;  
      }  
    }  
  }  
}
```

For more information about firewall filters, see the *Routing Policy Feature Guide for Routing Devices*; for more information about queuing, see the *Junos OS Class of Service Library for Routing Devices*.

**Related  
Documentation**

- [Real-Time Performance Monitoring Services Overview on page 1467](#)
- [\[edit services rpm\] Hierarchy Level on page 1471](#)
- [Examples: Configuring Real-Time Performance Monitoring on page 1516](#)

---

## Configuring TWAMP

You can configure the Two-Way Active Measurement Protocol (TWAMP) on all M Series and T Series routers that support Multiservices PICs (running in either Layer 2 or Layer 3 mode), and on MX Series routers. Only the responder (server) side of TWAMP is supported.



**NOTE:** TWAMP is not supported on PTX Series Packet Transport Routers.

For more information on TWAMP, see RFC 5357, *A Two-Way Active Measurement Protocol (TWAMP)*.

To configure TWAMP properties, include the **twamp** statement at the **[edit services rpm]** hierarchy level:

```
[edit services rpm]  
twamp {
```

```

server {
  client-list list-name {
    [ address address ];
  }
  authentication-mode mode;
  max-connection-duration hours;
  maximum-connections count;
  maximum-connections-per-client count;
  maximum-sessions count;
  maximum-sessions-per-connection count;
  port number;
  server-inactivity-timeout minutes;
}

```

The TWAMP configuration process includes the following tasks:

- [Configuring TWAMP Interfaces on page 1485](#)
- [Configuring TWAMP Servers on page 1485](#)

## Configuring TWAMP Interfaces

To specify the service PIC logical interface that provides the TWAMP service, include the **twamp-server** statement at the **[edit interfaces sp-fpc/pic/port unit logical-unit-number]** hierarchy level:

```
twamp-server;
```



**NOTE:** On MX Series routers that do not include a Multiservices DPC, you can configure the **twamp-server** statement on any interface (for example, **ge-1/0/1.10**). It is not necessary to configure this statement on a service interface (**sp-** or **ms-**) but you do need to include it in the configuration to activate the TWAMP reflector functionality.

## Configuring TWAMP Servers

You can specify a number of TWAMP server properties, some of which are optional, by including the **server** statement at the **[edit services rpm twamp]** hierarchy level:

```

[edit services rpm twamp]
server {
  client-list list-name {
    [ address address ];
  }
  authentication-mode mode;
  max-connection-duration hours;
  maximum-connections count;
  maximum-connections-per-client count;
  maximum-sessions count;
  maximum-sessions-per-connection count;
  port number;
  server-inactivity-timeout minutes;
}

```

- To specify the list of allowed control client hosts that can connect to this server, include the **client-list** statement at the **[edit services rpm twamp server]** hierarchy level. Each value you include must be a Classless Interdomain Routing (CIDR) address (IP address plus mask) that represents a network of allowed hosts. You can include multiple client lists, each of which can contain a maximum of 64 entries. You must configure at least one client address to enable TWAMP.
- You must specify the authentication mode by including the **authentication-mode** statement at the **[edit services rpm twamp server]** hierarchy level. There is no default value. You can configure **authenticated** or **encrypted** mode, based on RFC 4656; if there is no authentication or encryptions mode specified, you should set the value to **none**. This statement is required in the TWAMP configuration.
- To specify the inactivity timeout period in seconds, include the **inactivity-timeout** statement at the **[edit services rpm twamp server]** hierarchy level. By default, the value is **1800**; the range is 0 through 3600 seconds.
- To specify the maximum number of concurrent connections the server can have to client hosts, include the **maximum-connections** statement at the **[edit services rpm twamp server]** hierarchy level. The allowed range of values is 1 through 1000 and the default value is 64. You can also limit the number of connections the server can make to a particular client host by including the **maximum-connections-per-client** statement. The allowed range of values is 1 through 500 and the default value is 64.
- To specify the maximum number of sessions the server can have running at one time, include the **maximum-sessions** statement at the **[edit services rpm twamp server]** hierarchy level. The allowed range of values is 1 through 2048 and the default value is 64. You can also limit the number of sessions the server can have on a single connection by including the **maximum-sessions-per-connection** statement.
- To specify the TWAMP server listening port, include the **port** statement at the **[edit services rpm twamp server]** hierarchy level. The range is 1 through 65,535.
- To specify the server inactivity timeout period in minutes, include the **server-inactivity-timeout** statement at the **[edit services rpm twamp server]** hierarchy level. The range is 0 through 30 minutes.

---

## Enabling RPM for the Junos OS extension-provider package

Real-time performance monitoring (RPM), which has been supported on the adaptive services interface, is now supported by the Junos OS extension-provider package. RPM is supported on all platforms and service PICs that support the extension-provider package.



**NOTE:** In Junos OS releases earlier than 12.3, the extension provider package was variously known as MP-SDK, Junos Services Framework (JSF), and eJunos.

To enable RPM for the Junos OS extension-provider package on the adaptive services interface, configure the **object-cache-size**, **policy-db-size**, and **package** statements at the

[**edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider**] hierarchy level. For the extension-provider package, **package-name** in the **package package-name** statement is **jservices-rpm**.

For more information about the extension-provider package, see the *SDK Applications Configuration Guide and Command Reference*.

The following example shows how to enable RPM for the extension-provider package on the adaptive services interface:

```
chassis fpc 1 {
  pic 2 {
    adaptive-services {
      service-package {
        extension-provider {
          control-cores 1;
          data-cores 1;
          object-cache-size 512;
          policy-db-size 64;
          package jservices-rpm;
          syslog daemon any;
        }
      }
    }
  }
}
```

#### Related Documentation

- [Real-Time Performance Monitoring Services Overview on page 1467](#)
- [\[edit services rpm\] Hierarchy Level on page 1471](#)
- [Examples: Configuring Real-Time Performance Monitoring on page 1516](#)
- [destination-interface on page 1526](#)

## Tracing RPM Operations

Tracing operations track all RPM operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

By default, no events are traced. If you include the **traceoptions** statement at the [**edit services rpm**] hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called **rmopd** located in the **/var/log** directory.
- When the log file reaches 128 kilobytes (KB), it is renamed **rmopd.0**, then **rmopd.1**, and so on, until there are three trace files. Then the oldest trace file (**rmopd.2**) is overwritten. (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)
- Log files can be accessed only by the user who configures the tracing operation.

You can change this default behavior by using the **traceoptions** statements. Changing the defaults is described in the following sections:

1. [Configuring the RPM Log File Name on page 1488](#)
2. [Configuring the Number and Size of RPM Log Files on page 1488](#)
3. [Configuring Access to the Log File on page 1488](#)
4. [Configuring a Regular Expression for Lines to Be Logged on page 1488](#)
5. [Configuring the Trace Operations on page 1489](#)

## Configuring the RPM Log File Name

By default, the name of the file that records RPM trace output is **rmopd**. To specify a different file name:

```
[edit services rpm traceoptions]  
user@host set file filename
```

## Configuring the Number and Size of RPM Log Files

To configure the limits on the number and size of RPM trace files:

```
[edit services rpm traceoptions]  
user@host set file filename files number size size
```

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

For example, set the maximum file size to 2 MB, and the maximum number of files to 20 for a log file named **rpmtrace**:

```
[edit services rpm traceoptions]  
user@host set file rpmtrace files 20 size 2MB
```

When the **rpmtrace** file reaches 2 MB, it is renamed **rpmtrace.0**, and a new file called **rpmtrace** is created. When the new **rpmtrace** reaches 2 MB, **rpmtrace.0** is renamed **rpmtrace.1** and **rpmtrace** is renamed **rpmtrace.0**. This process repeats until there are 20 trace files. Then the oldest file (**rpmtrace.19**) is overwritten by **rpmtrace.18**.

## Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files:

```
[edit services rpm traceoptions]  
user@host set file filename world-readable
```

To explicitly set the default behavior:

```
[edit services rpm traceoptions]  
user@host set file filename no-world-readable
```

## Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

To refine the output by specifying a regular expression (regex) to be matched:

```
[edit services rpm traceoptions]
user@host set file filename match regular-expression
```

## Configuring the Trace Operations

By default, if the **traceoptions** configuration is present, only important events are logged. You can configure the trace operations to be logged by including the following statements at the **[edit services rpm traceoptions]** hierarchy level:

```
flag {
  all;
  configuration;
  error;
  ipc;
  ppm;
  statistics
}
```

Table 32 on page 758 describes the meaning of the RPM tracing flags.

Table 44: RPM Tracing Flags

Flag	Description	Default Setting
<b>all</b>	Trace all operations.	Off
<b>configuration</b>	Trace configuration events.	Off
<b>error</b>	Trace events related to catastrophic errors in daemon.	Off
<b>ipc</b>	Trace IPC events.	Off
<b>ppm</b>	Trace ppm events.	Off
<b>statistics</b>	Trace statistics.	Off

## Configuring an RFC 2544-Based Benchmarking Test

You can configure a benchmarking test to detect and measure performance attributes, such as throughput, latency, frame loss, and bursty or back-to-back frames, of network devices. RFC 2544-based benchmarking test is performed by transmitting test packets from a device that functions as the generator or the initiator. These packets are sent to a device that functions as the reflector, which receives and returns the packets back to the initiator.

You must configure a test profile and reference the test profile in a unique test name that defines the parameters for the test to be performed on a certain device. However, the test profile is required when the test mode is configured as initiation and termination. The **test-profile** parameter is disregarded when the test mode is configured as reflection. MX104 routers support only the reflection function in the RFC 2544-based benchmarking

tests. A reflection service does not use the parameters specified in the test profile because the reflection service it returns the frames to the initiator.

The following topics describe how to configure a test name for an RFC 2544-based benchmarking test on an MX104 router for Layer 3 IPv4 and Ethernet pseudowire networks:

- [Configuring a Test Name for an RFC 2544-Based Benchmarking Test for a IPv4 Network on page 1490](#)
- [Configuring a Test Name for an RFC 2544-Based Benchmarking Test for an Ethernet Pseudowire: on page 1491](#)

## Configuring a Test Name for an RFC 2544-Based Benchmarking Test for a IPv4 Network

You can configure a test name by including the **test-name test-name** statement at the **[edit services rpm rfc2544-benchmarking]** hierarchy level. In the test name, you can configure attributes of the test iteration, such as the address family (type of service, IPv4 or Ethernet), the logical interface, and test duration that are used for a benchmarking test to be run.

To configure a test name and define its attributes for an IPv4 network:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```
[edit]
user@host# edit services
```

2. Configure a instance.

```
[edit services]
user@host# edit rpm
```

3. Configure an RFC 2544-based benchmarking test for the RPM instance.

```
[edit services rpm]
user@host# edit rfc2544-benchmarking
```

4. Define a name for the test—for example, test1. The test name identifier can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name test1
```

5. Specify the test mode for the packets that are sent during the benchmarking test. The **reflect** option causes the test frames to be reflected on the IPv4 network.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set mode reflect
```

6. Configure the address type family for the benchmarking test. The **inet** option indicates that the test is run on an IPv4 service.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set family inet
```

7. Configure the destination IPv4 address for the test packets. This parameter is required only if you configure IPv4 family **inet**. If you do not configure the destination IPv4 address, the default value of 192.168.1.20 is used.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
```

```
user@host# set destination-ipv4-address address
```

8. Specify the UDP port of the destination to be used in the UDP header for the generated frames. If you do not specify the UDP port, the default value of 4041 is used.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set destination-udp-port port-number
```

9. (Optional) Specify the source IPv4 address to be used in generated test frames. If you do not configure the source IPv4 address for **inet** family, the source address of the interface is used to transmit the test frames.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set source-ipv4-address address
```

10. Specify the UDP port of the source to be used in the UDP header for the generated frames. If you do not specify the UDP port, the default value of 4041 is used.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set source-udp-port port-number
```

11. Specify the logical interface on which the RFC 2544-based benchmarking test is run. If you configure an **inet** family and the test mode to reflect the frames back on the sender from the other end, then the logical interface is used as the interface to enable the reflection service (reflection is performed on the packets entering the specified interface). If you not configure the logical interface for reflection test mode, then a lookup is performed on the source IPv4 address to determine the interface that hosts the address.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set test-interface interface-name
```

## Configuring a Test Name for an RFC 2544-Based Benchmarking Test for an Ethernet Pseudowire:

You can configure a test name by including the **test-name *test-name*** statement at the **[edit services rpm rfc2544-benchmarking]** hierarchy level. In the test name, you can configure attributes of the test iteration, such as the address family (type of service IPv4 or Ethernet), the logical interface, and test duration, that are used for a benchmarking test to be run. The test name combined with the test profile represent a single real-time performance monitoring (RPM) configuration instance.

To configure a test name and define its attributes for an Ethernet Pseudowire:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```
[edit]
user@host# edit services
```

2. Configure an RPM service instance.

```
[edit services]
user@host# edit rpm
```

3. Configure an RFC 2544-based benchmarking test for the RPM instance.

```
[edit services rpm]
user@host# edit rfc2544-benchmarking
```

4. Define a name for the test—for example, test1. The test name identifier can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name test1
```

5. Specify the test mode for the packets that are sent during the benchmarking test. The **reflect** option causes the test frames to be reflected on the Ethernet pseudowire.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set mode reflect
```

6. Configure the address type family for the benchmarking test. The **ccc** option indicates that the test is run on a CCC or Ethernet pseudowire service.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set family ccc
```

7. Specify the direction of the interface on which the test must be run. This parameter is valid only for a family. To enable the test to be run in the egress direction of the interface (network-to-network interface (NNI)), use the **egress** option. To enable the test to be run in the ingress direction of the interface (user-to-network interface (UNI)), use the **ingress** option.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set direction egress
```

8. (Optional) Specify the source IPv4 address to be used in generated test frames. If you do not configure the source IPv4 address for family, the default value of 192.168.1.10 is used.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set source-ipv4-address address
```

9. Specify the logical interface on which the RFC 2544-based benchmarking test is run.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set test-interface interface-name
```

#### Related Documentation

- [RFC 2544-Based Benchmarking Tests Overview on page 1468](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for UNI Direction of Ethernet Pseudowires on page 1500](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for NNI Direction of Ethernet Pseudowires on page 1507](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for Layer 3 IPv4 Services on page 1492](#)

### Example: Configuring an RFC 2544-Based Benchmarking Test for Layer 3 IPv4 Services

- [Requirements on page 1493](#)
- [Overview on page 1493](#)
- [Configuration on page 1493](#)
- [Verifying the Results of the Benchmarking Test for Layer 3 IPv4 Services on page 1499](#)

## Requirements

This example uses the following hardware and software components:

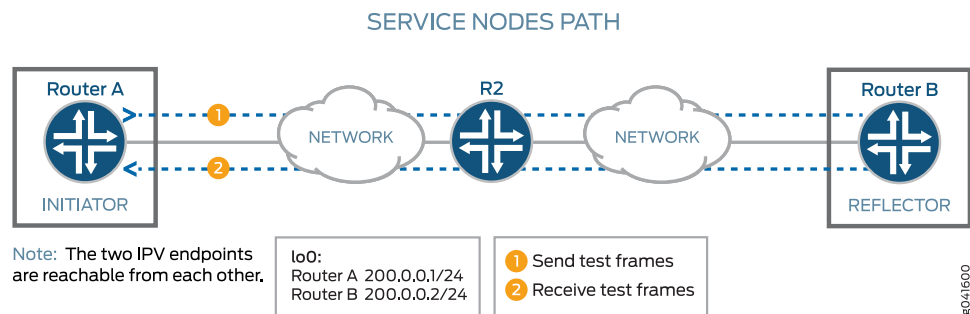
- 
- An ACX Series Universal Access Router—
- Junos OS Release or later

## Overview

Consider a sample topology in which a router, Router A, functions as an initiator and terminator of the test frames for an RFC 2544-based benchmarking test. Router A is connected over a Layer 3 network to another router, Router B, which functions as a reflector to reflect back the test frames it receives from Router A. IPv4 is used for transmission of test frames over the Layer 3 network. This benchmarking test is used to compute the IPv4 service parameters between Router A and Router B. Logical interfaces on both the routers are configured with IPv4 addresses to measure the performance attributes, such as throughput, latency, frame loss, and bursty frames, of network devices for the IPv4 service.

Figure 28 on page 1493 shows the sample topology to perform an RFC 2544 test for a Layer 3 IPv4 service.

**Figure 28: RFC 2544-Based Benchmarking Test for a Layer 3 IPv4 Service**



## Configuration

In this example, you configure the benchmarking test for a Layer 3 IPv4 service that is between interface ge-0/0/0 on Router A and interface ge-0/0/4 on Router B to detect and analyze the performance of the interconnecting routers.

- [Configuring Benchmarking Test Parameters on Router A on page 1494](#)
- [Configuring Benchmarking Test Parameters on Router B on page 1496](#)
- [Results on page 1498](#)

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level:

### Configuring Benchmarking Test Parameters on Router A

```
set interfaces ge-0/0/0 unit 0 family inet address 200.0.0.1/24
set interfaces ge-0/0/0 unit 0 family mpls
set rfc2544-benchmarking profiles test-profile throughput test-type throughput
set rfc2544-benchmarking profiles test-profile throughput packet-size 64
set rfc2544-benchmarking profiles test-profile throughput test-duration 20m
set rfc2544-benchmarking profiles test-profile throughput bandwidth-kbps 500
set rfc2544-benchmarking tests test-name test1 test-profile throughput
set rfc2544-benchmarking tests test-name test1 interface ge-0/0/0.1
set rfc2544-benchmarking tests test-name test1 mode initiate-and-terminate
set rfc2544-benchmarking tests test-name test1 family inet
set rfc2544-benchmarking tests test-name test1 dest-address 200.0.0.2
set rfc2544-benchmarking tests test-name test1 udp-port 4001
```

### Configuring Benchmarking Test Parameters on Router B

```
set interfaces ge-0/0/4 unit 0 family inet address 200.0.0.2/24
set interfaces ge-0/0/4 unit 0 family mpls
set services rpm rfc2544-benchmarking tests test-name test1 interface ge-0/0/4.1
set services rpm rfc2544-benchmarking tests test-name test1 mode reflect
set services rpm rfc2544-benchmarking tests test-name test1 family inet
set services rpm rfc2544-benchmarking tests test-name test1 dest-address 200.0.0.1
set services rpm rfc2544-benchmarking tests test-name test1 udp-port 4001
```

---

#### Configuring Benchmarking Test Parameters on Router A

---

##### Step-by-Step Procedure

The following require you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the test parameters on Router A:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level:

```
[edit]
user@host# edit interfaces
```

2. Configure the interface on which the test must be run.

```
[edit interfaces]
user@host# edit ge-0/0/0
```

3. Configure a logical unit and specify the protocol family.

```
[edit interfaces ge-0/0/0]
user@host# edit unit 0 family inet
```

4. Specify the address for the logical interface.

```
[edit interfaces ge-0/0/0 unit 0 family inet]
user@host# set address 200.0.0.1/24
```

5. Enter the **up** command to go the previous level in the configuration hierarchy.  

```
[edit interfaces ge-0/0/0 unit 0 family inet]
user@host# up
```
6. Configure the MPLS family on the logical interface.  

```
[edit interfaces ge-0/0/0 unit 0]
user@host# set family mpls
```
7. Go to the top level of the configuration command mode.  

```
[edit interfaces ge-0/0/0 unit 0]
user@host# top
```
8. In configuration mode, go to the **[edit services]** hierarchy level.  

```
[edit]
user@host# edit services
```
9. Configure a real-time performance monitoring service (RPM) instance.  

```
[edit services]
user@host# edit rpm
```
10. Configure an RFC 2544-based benchmarking test for the RPM instance.  

```
[edit services rpm]
user@host# edit rfc2544-benchmarking
```
11. Define a name for a test profile—for example, throughput.  

```
[edit services rpm rfc2544-benchmarking]
user@host# edit profiles test-profile throughput
```
12. Configure the type of test to be performed as throughput.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# set test-type throughput
```
13. Specify the size of the test packet as 64 bytes.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# set test-type packet-size 64
```
14. Specify the period for which the test is to be performed in hours, minutes, or seconds by specifying a number followed by the letter h (for hours), m (for minutes), or s (for seconds), respectively.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# set test-type test-duration 20m
```
15. Define the theoretical maximum bandwidth for the test in kilobits per second, with a value from 1 Kbps through 1,000,000 Kbps.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# set test-type bandwidth-kbps 500
```
16. Enter the **up** command to go the previous level in the configuration hierarchy.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# up
```
17. Enter the **up** command to go the previous level in the configuration hierarchy.

```
[edit services rpm rfc2544-benchmarking profiles]
user@host# up
```

18. Define a name for the test—for example, test1. The test name identifier can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name test1
```

19. Specify the name of the test profile—for example, throughput—to be associated with a particular test name.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set test-profile throughput
```

20. Specify the logical interface, ge-0/0/0.1, on which the RFC 2544-based benchmarking test is run.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set test-interface ge-0/0/0.1
```

21. Specify the test mode for the packets that are sent during the benchmarking test as initiation and termination.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set mode initiate-and-terminate
```

22. Configure the address type family, **inet**, for the benchmarking test.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set family inet
```

23. Configure the destination IPv4 address for the test packets.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set dest-address 200.0.0.2
```

24. Specify the UDP port of the destination to be used in the UDP header for the generated frames as 4001.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set udp-port 4001
```

25. Start the benchmarking test on the initiator.

```
user@> test services rpm rfc2544-benchmarking test test1 start
```

After the test is successfully completed, it is automatically stopped at the initiator.

---

### Configuring Benchmarking Test Parameters on Router B

#### Step-by-Step Procedure

The following you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the test parameters on Router B:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level:

```
[edit]
user@host# edit interfaces
```

2. Configure the interface on which the test must be run.  

```
[edit interfaces]  
user@host# edit ge-0/0/4
```
3. Configure a logical unit and specify the protocol family as **inet**.  

```
[edit interfaces ge-0/0/4]  
user@host# edit unit 0 family inet
```
4. Specify the address for the logical interface.  

```
[edit interfaces ge-0/0/4 unit 0 family inet]  
user@host# set address 200.0.0.2/24
```
5. Enter the **up** command to go the previous level in the configuration hierarchy.  

```
[edit interfaces ge-0/0/4 unit 0 family inet]  
user@host# up
```
6. Configure the MPLS family on the logical interface.  

```
[edit interfaces ge-0/0/4 unit 0]  
user@host# set family mpls
```
7. Go to the top level of the configuration command mode.  

```
[edit interfaces ge-0/0/4 unit 0]  
user@host# top
```
8. In configuration mode, go to the **[edit services]** hierarchy level.  

```
[edit]  
user@host# edit services
```
9. Configure a real-time performance monitoring service (RPM) instance.  

```
[edit services]  
user@host# edit rpm
```
10. Configure an RFC 2544-based benchmarking test for the RPM instance.  

```
[edit services rpm]  
user@host# edit rfc2544-benchmarking
```
11. Define a name for the test—for example, **test1**. The test name identifier can be up to 32 characters in length.  

```
[edit services rpm rfc2544-benchmarking]  
user@host# edit tests test-name test1
```
12. Specify the logical interface, **ge-0/0/4.1**, on which the RFC 2544-based benchmarking test is run.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set test-interface ge-0/0/4.1
```
13. Specify **reflect** as the test mode for the packets that are sent during the benchmarking test.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set mode reflect
```
14. Configure the address type family, **inet**, for the benchmarking test.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set family inet
```

15. Configure the destination IPv4 address for the test packets as 200.0.0.1.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set dest-address 200.0.0.1
```

16. Specify the UDP port of the destination to be used in the UDP header for the generated frames as 4001.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set udp-port 4001
```

17. Start the benchmarking test on the reflector.

```
user@host> test services rpm rfc2544-benchmarking test test1 start
```

After the test is successfully completed at the initiator, you can stop the test at the reflector by entering the **test services rpm rfc2544-benchmarking test test1** command.

---

## Results

In configuration mode, confirm your configuration on Router A and Router B by entering the **show** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

Benchmarking Test Parameters on Router A:

```
[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family inet {
      address 200.0.0.1/24;
    }
    family mpls;
  }
}

[edit services rpm]
rfc2544-benchmarking {
  profiles {
    test-profile throughput {
      test-type throughput
      packet-size 64;
      test-duration 20m;
      bandwidth-kbps 500;
    }
  }

  tests {
    test-name test1 {
      test-profile throughput;
      interface ge-0/0/0.1;
      mode initiate,terminate;
      family inet;
      dest-address 200.0.0.2
      udp-port 4001;
    }
  }
}
```

```
}

```

Benchmarking Test Parameters on Router B:

```
[edit interfaces]
ge-0/0/4 {
  unit 0 {
    family inet {
      address 200.0.0.2/24;
    }
    family mpls;
  }
}

[edit services rpm]
rfc2544-benchmarking {
  # Note, When in reflector mode, test profile is not needed
  tests {
    test-name test1 {
      interface ge-0/0/4.1;
      mode reflect;
      family inet;
      dest-address 200.0.0.1;
      udp-port 4001;
    }
  }
}
```

After you have configured the device, enter the **commit** command in configuration mode.

## Verifying the Results of the Benchmarking Test for Layer 3 IPv4 Services

Examine the results of the benchmarking test that is performed on the configured service between Router A and Router B.

- [Verifying the Benchmarking Test Results on page 1499](#)

### Verifying the Benchmarking Test Results

**Purpose** Verify that the necessary and desired statistical values are displayed for the benchmarking test that is run on the configured service between Router A and Router B.

**Action** In operational mode, enter the **show services rpm rfc2544-benchmarking (aborted-tests | active-tests | completed-tests | summary)** command to display information about the results of each category or state of the RFC 2544-based benchmarking test, such as aborted tests, active tests, and completed tests, for each real-time performance monitoring (RPM) instance.

**Related Documentation**

- [RFC 2544-Based Benchmarking Tests Overview on page 1468](#)
- [Configuring an RFC 2544-Based Benchmarking Test on page 1489](#)

## Example: Configuring an RFC 2544-Based Benchmarking Test for UNI Direction of Ethernet Pseudowires

---

This example shows how to configure the benchmarking test for the user-to-network interface (UNI) direction of an Ethernet pseudowire service.

- [Requirements on page 1500](#)
- [Overview on page 1500](#)
- [Configuration on page 1501](#)
- [Verifying the Results of the Benchmarking Test for UNI Direction of an Ethernet Pseudowire Service on page 1507](#)

### Requirements

This example uses the following hardware and software components:

- An ACX Series router—f
- Junos OS Release or later

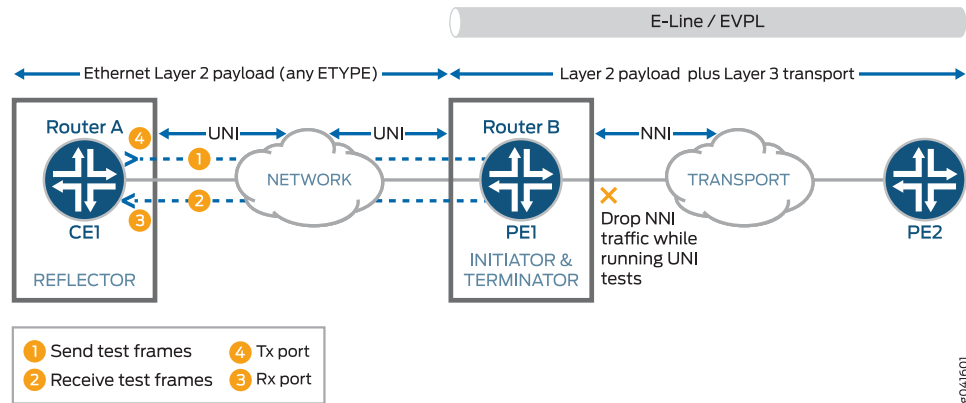
### Overview

Consider a sample topology in which a router, Router A, functions as a reflector of the test frames for an RFC 2544-based benchmarking test. The logical customer edge (CE)-facing interface and **inet** family are configured on Router A. Router A is not part of a pseudowire and therefore, a Layer 3 family configuration is required on it. Router A, which is a customer edge device CE1 is connected to Router B, which functions as a provider edge device PE1 over an Ethernet pseudowire in the UNI direction with EtherType or Layer 2 Ethernet payload. The logical interface, family, and UNI direction are configured on Router B. Router B or PE1 is connected over an Ethernet pseudowire in the NNI direction to a provider edge device at the remote site, PE2. The link between CE1 and PE1 is an Ethernet Layer 2 network and it can be configured with any EtherType value. The link between PE1 and PE2 is an Ethernet line (E-LINE) or an Ethernet Private Line (EPL) that has Layer 2 payload and Layer 3 transport sent over it. Router B or PE1 functions as an initiator and terminator of the test frames that are sent to Router A and reflected back from it.

This benchmarking test is used to compute the performance attributes in the user-to-network interface (UNI) direction of an Ethernet pseudowire service between Router A and Router B. Data traffic arriving from a network-to-network interface (NNI) toward the customer edge is ignored while the test is in progress. Packets from the CE are not sent toward the NNI because all packets are assumed to be test probes.

[Figure 29 on page 1501](#) shows the sample topology to perform an RFC 2544 test for the UNI direction of an Ethernet pseudowire service.

Figure 29: RFC 2544-Based Benchmarking Test for UNI Direction of an Ethernet Pseudowire



## Configuration

In this example, you configure the benchmarking test for the UNI direction of an Ethernet pseudowire service that is enabled between two routers to detect and analyze the performance of the interconnecting routers.

- [Configuring Benchmarking Test Parameters on Router A on page 1502](#)
- [Configuring Benchmarking Test Parameters on Router B on page 1504](#)
- [Results on page 1505](#)

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level:

### Configuring Benchmarking Test Parameters on Router A

```
set interfaces ge-0/0/0 vlan-tagging
set interfaces ge-0/0/0 unit 0 vlan-id 101
set interfaces ge-0/0/0 unit 0 family inet address 200.0.0.1/24
set services rpm rfc2544-benchmarking profiles test-profile throughput test-type throughput
set services rpm rfc2544-benchmarking profiles test-profile throughput packet-size 64
set services rpm rfc2544-benchmarking profiles test-profile throughput test-duration 20m
set services rpm rfc2544-benchmarking profiles test-profile throughput bandwidth-kbps 500
set services rpm rfc2544-benchmarking tests test-name test1 interface ge-0/0/0.1
set services rpm rfc2544-benchmarking tests test-name test1 test-profile throughput
set services rpm rfc2544-benchmarking tests test-name test1 mode initiate,terminate
set services rpm rfc2544-benchmarking tests test-name test1 family inet
set services rpm rfc2544-benchmarking tests test-name test1 dest-address 200.0.0.2
set services rpm rfc2544-benchmarking tests test-name test1 udp-port 4001
```

## Configuring Benchmarking Test Parameters on Router B

```
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 0 encapsulation vlan-ccc
set interfaces ge-0/0/4 unit 0 vlan-id 101
set services rpm rfc2544-benchmarking tests test-name test1 interface ge-0/0/4.1
set services rpm rfc2544-benchmarking tests test-name test1 mode reflect
set services rpm rfc2544-benchmarking tests test-name test1 mode family ccc
set services rpm rfc2544-benchmarking tests test-name test1 direction uni
```

---

### Configuring Benchmarking Test Parameters on Router A

#### Step-by-Step Procedure

The following require you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the test parameters on Router A:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level:  

```
[edit]
user@host# edit interfaces
```
2. Configure the interface on which the test must be run.  

```
[edit interfaces]
user@host# edit ge-0/0/0
```
3. Configure VLAN tagging for transmission and reception of 802.1Q VLAN-tagged frames.  

```
[edit interfaces ge-0/0/0]
user@host# set vlan-tagging
```
4. Configure a logical unit and specify the protocol family as **inet**.  

```
[edit interfaces ge-0/0/0]
user@host# edit unit 0 family inet
```
5. Specify the address for the logical interface.  

```
[edit interfaces ge-0/0/0 unit 0 family inet]
user@host# set address 200.0.0.1/24
```
6. Configure the VLAN ID on the logical interface as 101.  

```
[edit interfaces ge-0/0/0 unit 0]
user@host# set vlan-id 101
```
7. Go to the top level of the configuration command mode.  

```
[edit interfaces ge-0/0/0 unit 0]
user@host# top
```
8. In configuration mode, go to the **[edit services]** hierarchy level.  

```
[edit]
user@host# edit services
```

9. Configure a real-time performance monitoring service (RPM) instance.  

```
[edit services]
user@host# edit rpm
```
10. Configure an RFC 2544-based benchmarking test for the RPM instance.  

```
[edit services rpm]
user@host# edit rfc2544-benchmarking
```
11. Define a name for a test profile—for example, throughput.  

```
[edit services rpm rfc2544-benchmarking]
user@host# edit profiles test-profile throughput
```
12. Configure the type of test to be performed as throughput.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# set test-type throughput
```
13. Specify the size of the test packet as 64 bytes.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# set test-type packet-size 64
```
14. Specify the period for which the test is to be performed in hours, minutes, or seconds by specifying a number followed by the letter h (for hours), m (for minutes), or s (for seconds). In this example, you configure the period as 20 minutes.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# set test-type test-duration 20m
```
15. Define the theoretical maximum bandwidth for the test in kilobits per second, with a value from 1 Kbps through 1,000,000 Kbps.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# set test-type bandwidth-kbps 500
```
16. Enter the **up** command to go the previous level in the configuration hierarchy.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# up
```
17. Enter the **up** command to go the previous level in the configuration hierarchy.  

```
[edit services rpm rfc2544-benchmarking profiles]
user@host# up
```
18. Define a name for the test—for example, test1. The test name identifier can be up to 32 characters in length.  

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name test1
```
19. Specify the name of the test profile—for example, throughput—to be associated with a particular test name.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set test-profile throughput
```
20. Specify the logical interface, ge-0/0/0.1, on which the RFC 2544-based benchmarking test is run.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
```

```
user@host# set test-interface ge-0/0/0.1
```

21. Specify the test mode for the packets that are sent during the benchmarking test as initiation and termination.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set mode initiate-and-terminate
```

22. Configure the address type family, **inet**, for the benchmarking test.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set family inet
```

23. Configure the destination IPv4 address for the test packets as 200.0.0.2.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set dest-address 200.0.0.2
```

24. Specify the UDP port of the destination to be used in the UDP header for the generated frames as 4001.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set udp-port 4001
```

---

### Configuring Benchmarking Test Parameters on Router B

#### Step-by-Step Procedure

The following require you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the test parameters on Router B:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level:

```
[edit]  
user@host# edit interfaces
```

2. Configure the interface on which the test must be run.

```
[edit interfaces]  
user@host# edit ge-0/0/4
```

3. Configure VLAN tagging for transmission and reception of 802.1Q VLAN-tagged frames.

```
[edit interfaces ge-0/0/4]  
user@host# set vlan-tagging
```

4. Configure a logical unit for the interface.

```
[edit interfaces ge-0/0/4]  
user@host# edit unit 0
```

5. Specify the encapsulation for Ethernet VLAN circuits.

```
[edit interfaces ge-0/0/4 unit 0]  
user@host# set encapsulation vlan-ccc
```

6. Configure the VLAN ID as 101 on the logical interface.

```
[edit interfaces ge-0/0/4 unit 0]  
user@host# set vlan-id 101
```

7. Go to the top level of the configuration command mode.  

```
[edit interfaces ge-0/0/4 unit 0]  
user@host# top
```
8. In configuration mode, go to the **[edit services]** hierarchy level.  

```
[edit]  
user@host# edit services
```
9. Configure a real-time performance monitoring service (RPM) instance.  

```
[edit services]  
user@host# edit rpm
```
10. Configure an RFC 2544-based benchmarking test for the RPM instance.  

```
[edit services rpm]  
user@host# edit rfc2544-benchmarking
```
11. Define a name for the test—for example, test1. The test name identifier can be up to 32 characters in length.  

```
[edit services rpm rfc2544-benchmarking]  
user@host# edit tests test-name test1
```
12. Specify the logical interface on which the RFC 2544-based benchmarking test is run.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set test-interface ge-0/0/4.1
```
13. Specify **reflect** as the test mode for the packets that are sent during the benchmarking test.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set mode reflect
```
14. Configure the address type family, **ccc**, for the benchmarking test.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set family ccc
```
15. Specify the direction of the interface on which the test must be run, which is UNI in this example.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set direction uni
```

---

## Results

In configuration mode, confirm your configuration on Router A and Router B by entering the **show** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

Benchmarking Test Parameters on Router A:

```
[edit interfaces]  
ge-0/0/0 {  
  vlan-tagging;  
  unit 0 {
```

```
        vlan-id 101;
        family inet {
            address 200.0.0.1/24;
        }
    }

[edit services rpm]
rfc2544-benchmarking {
    profiles {
        test-profile throughput {
            test-type throughput
            packet-size 64;
            test-duration 20m;
            bandwidth-kbps 500;
        }
    }

    tests {
        test-name test1 {
            interface ge-0/0/0.1;
            test-profile throughput;
            mode initiate,terminate;
            family inet;
            dest-address 200.0.0.2
            udp-port 4001;
        }
    }
}
```

#### Benchmarking Test Parameters on Router B:

```
[edit interfaces]
ge-0/0/4 {
    vlan-tagging;
    unit 0 {
        encapsulation vlan-ccc;
        vlan-id 101;
    }
}

[edit services rpm]
rfc2544-benchmarking {
    # Note, When in reflector mode, test profile is not needed
    tests {
        test-name test1 {
            interface ge-0/0/4.1;
            mode reflect;
            family ccc;
            direction uni;
        }
    }
}
```

After you have configured the device, enter the **commit** command in configuration mode.

## Verifying the Results of the Benchmarking Test for UNI Direction of an Ethernet Pseudowire Service

Examine the results of the benchmarking test that is performed on the configured service between Router A and Router B.

- [Verifying the Benchmarking Test Results on page 1507](#)

---

### Verifying the Benchmarking Test Results

**Purpose** Verify that the necessary and desired statistical values are displayed for the benchmarking test that is run on the configured service between Router A and Router B.

**Action** In operational mode, enter the **show services rpm rfc2544-benchmarking (aborted-tests | active-tests | completed-tests | summary)** command to display information about the results of each category or state of the RFC 2544-based benchmarking test, such as aborted tests, active tests, and completed tests, for each real-time performance monitoring (RPM) instance.

**Meaning** The output displays the details of the benchmarking test that was performed. For more information about the **show services rpm rfc2544-benchmarking** operational command, see **show services rpm rfc2544-benchmarking** in the [CLI Explorer](#).

**Related Documentation**

- [RFC 2544-Based Benchmarking Tests Overview on page 1468](#)
- [Configuring an RFC 2544-Based Benchmarking Test on page 1489](#)

---

## Example: Configuring an RFC 2544-Based Benchmarking Test for NNI Direction of Ethernet Pseudowires

This example shows how to configure the benchmarking test for a network-to-network interface (NNI) direction of an Ethernet pseudowire service.

- [Requirements on page 1507](#)
- [Overview on page 1508](#)
- [Configuration on page 1508](#)
- [Verifying the Results of the Benchmarking Test for NNI Direction of an Ethernet Pseudowire Service on page 1514](#)

### Requirements

This example uses the following hardware and software components:

- An ACX Series router
- Junos OS Release or later

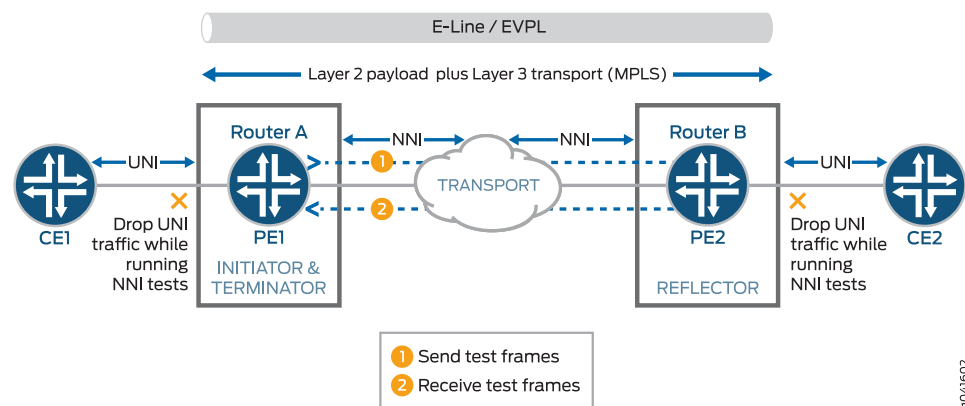
## Overview

Consider a sample topology in which a router, Router A, functions as an initiator and terminator of the test frames for an RFC 2544-based benchmarking test. Router A operates as a provider edge device PE1, which is connected to a customer edge device CE1 on one side and over an Ethernet pseudowire to another router Router B, which functions as a reflector to reflect back the test frames it receives from Router A. Router B operates as a provider edge device, PE2, which is the remote router located at the other side of the service provider core. The UNI direction of CE1 is connected to the NNI direction of PE1. An MPLS tunnel connects PE1 and PE2 over the Ethernet pseudowire or the Ethernet line (E-LINE).

This benchmarking test is used to compute the performance attributes in the network-to-network interface (NNI) direction of an Ethernet pseudowire service between Router A and Router B. The logical interface under test on Router A is the CE1 interface with UNI as the direction, and the logical interface under test on Router B is the CE2 interface with NNI as the direction. Data traffic arriving from UNI toward NNI is ignored while the test is in progress. Packets from NNI are not sent toward the customer edge because all packets are assumed to be test frames. The family and NNI direction are configured on routers A and B.

Figure 30 on page 1508 shows the sample topology to perform an RFC 2544 test for the NNI direction of an Ethernet pseudowire service.

**Figure 30: RFC 2544-Based Benchmarking Test for NNI Direction of an Ethernet Pseudowire**



## Configuration

In this example, you configure the benchmarking test for the NNI direction of an Ethernet pseudowire service that is enabled between two routers to detect and analyze the performance of the interconnecting routers.

- [Configuring Benchmarking Test Parameters on Router on page 1509](#)
- [Configuring Benchmarking Test Parameters on Router B on page 1511](#)
- [Results on page 1513](#)

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level:

**Configuring  
Benchmarking Test  
Parameters on Router  
A**

```
set interfaces ge-0/0/0 vlan-tagging
set interfaces ge-0/0/0 unit 0 encapsulation vlan-ccc
set interfaces ge-0/0/0 unit 0 vlan-id 101
set services rpm rfc2544-benchmarking profiles test-profile throughput test-type
throughput
set services rpm rfc2544-benchmarking profiles test-profile throughput packet-size 64
set services rpm rfc2544-benchmarking profiles test-profile throughput test-duration 20
set services rpm rfc2544-benchmarking profiles test-profile throughput bandwidth-kbps
500
set services rpm rfc2544-benchmarking tests test-name test1 interface ge-0/0/0.1
set services rpm rfc2544-benchmarking tests test-name test1 test-profile throughput
set services rpm rfc2544-benchmarking tests test-name test1 mode initiate,terminate
set services rpm rfc2544-benchmarking tests test-name test1 family ccc
set services rpm rfc2544-benchmarking tests test-name test1 direction nni
```

**Configuring  
Benchmarking Test  
Parameters on Router  
B**

```
set interfaces ge-0/0/4 vlan-tagging
set interfaces ge-0/0/4 unit 0 encapsulation vlan-ccc
set interfaces ge-0/0/4 unit 0 vlan-id 101
set services rpm rfc2544-benchmarking tests test-name test1 interface ge-0/0/4.1
set services rpm rfc2544-benchmarking tests test-name test1 mode reflect
set services rpm rfc2544-benchmarking tests test-name test1 mode family ccc
set services rpm rfc2544-benchmarking tests test-name test1 direction uni
```

### Configuring Benchmarking Test Parameters on Router

**Step-by-Step Procedure**

The following require you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the test parameters on Router A:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level:

```
[edit]
user@host# edit interfaces
```

2. Configure the interface on which the test must be run.

```
[edit interfaces]
user@host# edit ge-0/0/0
```

3. Configure VLAN tagging for transmission and reception of 802.1Q VLAN-tagged frames.

```
[edit interfaces ge-0/0/0]  
user@host# set vlan-tagging
```

4. Configure a logical unit for the interface.

```
[edit interfaces ge-0/0/0]  
user@host# edit unit 0
```

5. Specify the encapsulation for Ethernet VLAN circuits.

```
[edit interfaces ge-0/0/0 unit 0]  
user@host# set encapsulation vlan-ccc
```

6. Configure the VLAN ID on the logical interface.

```
[edit interfaces ge-0/0/0 unit 0]  
user@host# set vlan-id 101
```

7. Go to the top level of the configuration command mode.

```
[edit interfaces ge-0/0/0 unit 0]  
user@host# top
```

8. In configuration mode, go to the **[edit services]** hierarchy level.

```
[edit]  
user@host# edit services
```

9. Configure a real-time performance monitoring service (RPM) instance.

```
[edit services]  
user@host# edit rpm
```

10. Configure an RFC 2544-based benchmarking test for the RPM instance.

```
[edit services rpm]  
user@host# edit rfc2544-benchmarking
```

11. Define a name for a test profile—for example, throughput.

```
[edit services rpm rfc2544-benchmarking]  
user@host# edit profiles test-profile throughput
```

12. Configure the type of test to be performed as throughput.

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]  
user@host# set test-type throughput
```

13. Specify the size of the test packet as 64 bytes.

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]  
user@host# set test-type packet-size 64
```

14. Specify the period—for example, 20 minutes—for which the test is to be performed in hours, minutes, or seconds by specifying a number followed by the letter h (for hours), m (for minutes), or s (for seconds).

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]  
user@host# set test-type test-duration 20m
```

15. Define the theoretical maximum bandwidth for the test in kilobits per second, with a value from 1 Kbps through 1,000,000 Kbps.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# set test-type bandwidth-kbps 500
```
16. Enter the **up** command to go the previous level in the configuration hierarchy.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile throughput]
user@host# up
```
17. Enter the **up** command to go the previous level in the configuration hierarchy.  

```
[edit services rpm rfc2544-benchmarking profiles]
user@host# up
```
18. Define a name for the test—for example, test1. The test name identifier can be up to 32 characters in length.  

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name test1
```
19. Specify the name of the test profile—for example, throughput—to be associated with a particular test name.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set test-profile throughput
```
20. Specify the logical interface, ge-0/0/0.1, on which the RFC 2544-based benchmarking test is run.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set test-interface ge-0/0/0.1
```
21. Specify the test mode for the packets that are sent during the benchmarking test as initiation and termination.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set mode initiate-and-terminate
```
22. Configure the address type family, **ccc**, for the benchmarking test.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set family ccc
```
23. Specify the direction of the interface on which the test must be run, which is NNI in this example.  

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set direction nni
```

### Configuring Benchmarking Test Parameters on Router B

#### Step-by-Step Procedure

The following require you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the test parameters on Router B:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level:

- [edit]  
user@host# edit interfaces
2. Configure the interface on which the test must be run.
- [edit interfaces]  
user@host# edit ge-0/0/4
3. Configure VLAN tagging for transmission and reception of 802.1Q VLAN-tagged frames.
- [edit interfaces ge-0/0/4]  
user@host# set vlan-tagging
4. Configure a logical unit for the interface.
- [edit interfaces ge-0/0/4]  
user@host# edit unit 0
5. Specify the encapsulation for Ethernet VLAN circuits.
- [edit interfaces ge-0/0/4 unit 0]  
user@host# set encapsulation vlan-ccc
6. Configure the VLAN ID on the logical interface.
- [edit interfaces ge-0/0/4 unit 0]  
user@host# set vlan-id 101
7. Go to the top level of the configuration command mode.
- [edit interfaces ge-0/0/4 unit 0]  
user@host# top
8. In configuration mode, go to the **[edit services]** hierarchy level.
- [edit]  
user@host# edit services
9. Configure a real-time performance monitoring service (RPM) instance.
- [edit services]  
user@host# edit rpm
10. Configure an RFC 2544-based benchmarking test for the RPM instance.
- [edit services rpm]  
user@host# edit rfc2544-benchmarking
11. Define a name for the test—for example, test1. The test name identifier can be up to 32 characters in length.
- [edit services rpm rfc2544-benchmarking]  
user@host# edit tests test-name test1
12. Specify the logical interface, ge-0/0/4.1, on which the RFC 2544-based benchmarking test is run.
- [edit services rpm rfc2544-benchmarking tests test-name test1]  
user@host# set test-interface ge-0/0/4.1
13. Specify **reflect** as the test mode for the packets that are sent during the benchmarking test.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set mode reflect
```

14. Configure the address type family, **ccc**, for the benchmarking test.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set family ccc
```

15. Specify the direction of the interface on which the test must be run, which is **NNI** in this example.

```
[edit services rpm rfc2544-benchmarking tests test-name test1]
user@host# set direction nni
```

## Results

In configuration mode, confirm your configuration on Router A and Router B by entering the **show** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

Benchmarking Test Parameters on Router A:

```
[edit interfaces]
ge-0/0/0 {
  vlan-tagging;
  unit 0 {
    encapsulation vlan-ccc;
    vlan-id 101;
  }
}

[edit services rpm]
rfc2544-benchmarking {
  profiles {
    test-profile throughput {
      test-type throughput
      packet-size 64;
      test-duration 20m;
      bandwidth-kbps 500;
    }
  }

  tests {
    test-name test1 {
      interface ge-0/0/0.1;
      test-profile throughput;
      mode initiate,terminate;
      family ccc;
      direction nni;
    }
  }
}
```

Benchmarking Test Parameters on Router B:

```
[edit interfaces]
ge-0/0/4 {
  vlan-tagging;
```

```

        unit 0 {
            encapsulation vlan-ccc;
            vlan-id 101;
        }
    }

    [edit services rpm]
    rfc2544-benchmarking {
        # Note, When in reflector mode, test profile is not needed
        tests {
            test-name test1 {
                interface ge-0/0/4.1;
                mode reflect;
                family ccc;
                direction nni;
            }
        }
    }
}

```

After you have configured the device, enter the **commit** command in configuration mode.

## Verifying the Results of the Benchmarking Test for NNI Direction of an Ethernet Pseudowire Service

Examine the results of the benchmarking test that is performed on the configured service between Router A and Router B.

- [Verifying the Benchmarking Test Results on page 1514](#)

### Verifying the Benchmarking Test Results

<b>Purpose</b>	Verify that the necessary and desired statistical values are displayed for the benchmarking test that is run on the configured service between Router A and Router B.
<b>Action</b>	In operational mode, enter the <b>show services rpm rfc2544-benchmarking (aborted-tests   active-tests   completed-tests   summary)</b> command to display information about the results of each category or state of the RFC 2544-based benchmarking test, such as aborted tests, active tests, and completed tests, for each real-time performance monitoring (RPM) instance.
<b>Meaning</b>	The output displays the details of the benchmarking test that was performed. For more information about the <b>show services rpm rfc2544-benchmarking</b> operational command, see <b>show services rpm rfc2544-benchmarking</b> in the <a href="#">CLI Explorer</a> .
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li> <li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li> </ul>

## Examples: Configuring BGP Neighbor Discovery Through RPM

Configure BGP neighbor discovery through RPM for all logical systems and all routing instances:

```
[edit services rpm]
bgp {
  probe-type icmp-ping;
  probe-count 5;
  probe-interval 1;
  test-interval 60;
  history-size 10;
  data-size 255;
  data-fill 0123456789;
}
```

Configure BGP neighbor discovery through RPM for only the following logical systems and routing instances: **LS1/RI1**, **LS1/RI2**, **LS2**, and **RI3**:

```
[edit services rpm]
bgp {
  probe-type icmp-ping;
  probe-count 5;
  probe-interval 1;
  test-interval 60;
  history-size 10;
  data-size 255;
  data-fill 0123456789;
  logical-system {
    LS1 {
      routing-instances {
        RI1;
        RI2;
      }
    }
    LS2;
  }
  routing-instance {
    RI3;
  }
}
```



**NOTE:** The `logical-system` statement is not supported on PTX Series Packet Transport Routers.

Configure BGP neighbor discovery through RPM for only the default logical system and default routing instance:

```
[edit services rpm]
bgp {
  probe-type icmp-ping;
  probe-count 5;
  probe-interval 1;
```

```
test-interval 60;
history-size 10;
data-size 255;
data-fill 0123456789;
logical-system {
  null {
    routing-instances {
      default;
    }
  }
}
```

**Related  
Documentation**

- [Real-Time Performance Monitoring Services Overview on page 1467](#)
- [Configuring BGP Neighbor Discovery Through RPM on page 1473](#)
- [\[edit services rpm\] Hierarchy Level on page 1471](#)

---

## Examples: Configuring Real-Time Performance Monitoring

Configure an RPM instance identified by the probe name **probe1** and the test name **test1**:

```
[edit services rpm]
probe probe1 {
  test test1 {
    dscp-code-points 001111;
    probe-interval 1;
    probe-type icmp-ping;
    target address 172.17.20.182;
    test-interval 20;
    thresholds rtt 10;
    traps rtt-exceeded;
  }
}
probe-server {
  tcp {
    destination-interface lt-0/0/0.0
    port 50000;
  }
  udp {
    destination-interface lt-0/0/0.0
    port 50001;
  }
}
probe-limit 200;
```

Configure packet classification, using **lt-** interfaces to send the probe packets to a logical tunnel input interface. By sending the packet to the logical tunnel interface, you can configure regular and multifield classifiers, firewall filters, and header rewriting for the probe packets. To use the existing tunnel framework, the **dlci** and **encapsulation** statements must be configured.

```
[edit services rpm]
probe p1 {
  test t1 {
```

```

    probe-type icmp-ping;
    target address 10.8.4.1;
    probe-count 10;
    probe-interval 10;
    test-interval 10;
    source-address 10.8.4.2;
    dscp-code-points ef;
    data-size 100;
    destination-interface lt-0/0/0.0;
  }
}
[edit interfaces]
lt-0/0/0 {
  unit 0 {
    encapsulation frame-relay;
    dlci 10;
    peer-unit 1;
    family inet;
  }
  unit 1 {
    encapsulation frame-relay;
    dlci 10;
    peer-unit 0;
    family inet;
  }
}
[edit class-of-service]
interfaces {
  lt-0/0/0 {
    unit 1 {
      classifiers {
        dscp default;
      }
    }
  }
}

```

Configure an input filter on the interface on which the RPM probes are received. This filter enables prioritization of the received RPM packets, separating them from the regular data packets received on the same interface.

```

[edit firewall]
filter recos {
  term recos {
    from {
      source-address {
        10.8.4.1/32;
      }
      destination-address {
        10.8.4.2/32;
      }
    }
    then {
      loss-priority high;
      forwarding-class network-control;
    }
  }
}

```

```
    }  
  }  
[edit interfaces]  
fe-5/0/0 {  
  unit 0 {  
    family inet {  
      filter {  
        input recos;  
      }  
      address 10.8.4.2/24;  
    }  
  }  
}
```

Configure an RPM instance and enable RPM for the extension-provider packages on the adaptive services interface:

```
[edit services rpm]  
probe probe1 {  
  test test1 {  
    data-size 1024;  
    data-fill 0;  
    destination-interface ms-1/2/0.10;  
    dscp-code-points 001111;  
    probe-count 10;  
    probe-interval 1;  
    probe-type icmp-ping;  
    target address 172.17.20.182;  
    test-interval 20;  
    thresholds rtt 10;  
    traps rtt-exceeded;  
  }  
}  
[edit interfaces]  
ms-1/2/0 {  
  unit 0 {  
    family inet;  
  }  
  unit 10 {  
    rpm client;  
    family inet {  
      address 1.1.1.1/32;  
    }  
  }  
}  
[edit chassis]  
fpc 1 {  
  pic 2 {  
    adaptive-services {  
      service-package {  
        extension-provider {  
          control-cores 1;  
          data-cores 1;  
          object-cache-size 512;  
          policy-db-size 64;  
          package jservices-rpm;  
          syslog {
```

```

        daemon any;
    }
}
}
}
}
}

```



**NOTE:** TWAMP is not supported on PTX Series Packet Transport Routers.

Configure the minimum statements necessary to enable TWAMP:

```

[edit services]
rpm {
  twamp {
    server {
      authentication-mode none;
      port 10000; # Twamp server's listening port
      client-list LIST-1 { # LIST-1 is the name of the client-list. Multiple lists can be
        configured.
        address {
          20.0.0.2/30; # IP address of the control client.
        }
      }
    }
  }
}
[edit interfaces sp-5/0/0]
unit 0 {
  family inet;
}
unit 10 {
  rpm {
    twamp-server; # You must configure a separate logical interface on the service PIC
    interface for the TWAMP server.
  }
  family inet {
    address 50.50.50.50/32; # This address must be a host address with a 32-bit mask.
  }
}
[edit chassis]
fpc 5 {
  pic 0 {
    adaptive-services {
      service-package layer-2; # Configure the service PIC to run in Layer 2 mode.
    }
  }
}
}

```

Configure additional TWAMP settings:

```

[edit services]
rpm {
  twamp {
    server {
      maximum-sessions 5;
    }
  }
}

```

```
maximum-sessions-per-connection 2;
maximum-connections 3;
maximum-connections-per-client 1;
port 10000;
server-inactivity-timeout ;
client-list LIST-1 {
    address {
        20.0.0.2/30;
    }
}
}
```

**Related  
Documentation**

- [Real-Time Performance Monitoring Services Overview on page 1467](#)
- [\[edit services rpm\] Hierarchy Level on page 1471](#)
- [Examples: Configuring BGP Neighbor Discovery Through RPM on page 1515](#)

## CHAPTER 62

# Summary of Real-Time Performance Monitoring Configuration Statements

The following sections explain each of the Real-Time Performance Monitoring (RPM) statements. The statements are organized alphabetically.

### authentication-mode

---

<b>Syntax</b>	authentication-mode (authenticated   control-only-encrypted   encrypted   none);
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm twamp server]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the authentication or encryption mode support for the TWAMP test protocol. This statement is required in the configuration; if no authentication or encryption is specified, you should set the value to <b>none</b> .
<b>Options</b>	<b>authenticated</b> —Data packets are authenticated.  <b>control-only-encrypted</b> —TWAMP control packets are encrypted. TWAMP data packets are in plain text format.  <b>encrypted</b> —Data packets are encrypted.  <b>none</b> —No authentication or encryption.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## bgp

---

**Syntax**    `bgp {  
          data-fill data;  
          data-size size;  
          destination-port port;  
          history-size size;  
          logical-system logical-system-name <routing-instances routing-instance-name>;  
          moving-average-size size;  
          probe-count count;  
          probe-interval seconds;  
          probe-type type;  
          routing-instances instance-name;  
          test-interval interval;  
          }`

**Hierarchy Level**    `[edit services rpm bgp]  
                      [edit protocols bgp group group-name]  
                      [edit routing-instances instance-name protocols bgp group group-name]  
                      [edit logical-system logical-system-name protocols bgp group group-name]  
                      [edit logical-system logical-system-name routing-instances instance-name protocols bgp  
                          group group-name]`

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure BGP neighbor discovery through Real-Time Performance Monitoring (RPM).

**Options**    **bgp**—Define properties for configuring BGP neighbor discovery.

The remaining statements are explained separately.



**NOTE:** On MX Series routers, you can configure all the statements. On M Series and T Series routers, you can configure only the `logical-system` and `routing-instances` statements.

---

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring BGP Neighbor Discovery Through RPM on page 1473](#)

## client-list

---

<b>Syntax</b>	<code>client-list <i>list-name</i> {     address <i>address</i>; }</code>
<b>Hierarchy Level</b>	[edit services rpm twamp server]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	List of allowed control client hosts that can connect to this server. Each entry is a Classless Interdomain Routing (CIDR) address (IP address plus mask) that represents a network of allowed hosts. You can configure more than one list, but you must configure at least one client address to enable TWAMP. Each list can contain up to 64 entries.
<b>Options</b>	<i>list-name</i> —Name of client address list.  <i>address</i> —Address and mask for an allowed client.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring TWAMP on page 1484</a></li> </ul>

## data-fill

---

<b>Syntax</b>	<code>data-fill <i>data</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm bgp], [edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 9.3 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the contents of the data portion of Internet Control Message Protocol (ICMP) probes. The <b>data-fill</b> statement is not valid with the <b>http-get</b> or <b>http-metadata-get</b> probe types.
<b>Options</b>	<i>data</i> —A hexadecimal value; for example, 0-9, A-F.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li> <li>• <a href="#">Configuring RPM Probes on page 1475</a></li> </ul>

## data-size

---

Syntax	<code>data-size size;</code>
Hierarchy Level	[edit services rpm bgp], [edit <b>services</b> rpm <b>probe</b> owner <b>test</b> test-name]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
Description	Specify the size of the data portion of ICMP probes. The <b>data-size</b> statement is not valid with the <b>http-get</b> or <b>http-metadata-get</b> probe type.
Options	<b>data</b> —The size can be from 0 through 65400 <b>Default:</b> 0



**NOTE:** If you configure the hardware timestamp feature (see [“Configuring RPM Timestamping” on page 1481](#)):

- The **data-size** default value is 32 bytes and 32 is the minimum value for explicit configuration. The UDP timestamp probe type is an exception; it requires a minimum data size of 52 bytes.
  - The **data-size** must be at least 100 bytes smaller than the default MTU of the interface of the RPM client interface.
- 

Required Privilege Level	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li></ul>

## destination-ipv4-address (RFC 2544 Benchmarking)

---

<b>Syntax</b>	<code>destination-ipv4-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> <i>test-name</i> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X52 for ACX Series routers. Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.
<b>Description</b>	Specify the destination IPv4 address to be used in generated test frames. You must configure this option if you specify <code>inet</code> as the family. This option is not required if you specify <code>cccas</code> the family.
<b>Options</b>	<b><i>address</i></b> —Valid IPv4 address. <b>Default:</b> If you do not configure the destination IPv4 address, the default value of 192.168.1.20 is used.
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li><li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li><li>• <a href="#">rfc2544-benchmarking on page 1544</a></li></ul>

## destination-interface

---

Syntax	<code>destination-interface <i>interface-name</i>;</code>
Hierarchy Level	[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> <i>test-name</i> ], [edit services rpm probe-server ( <a href="#">tcp</a>   <a href="#">udp</a> )]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	<p>On M Series and T Series routers, specify a services (<b>sp-</b>) interface that adds a timestamp to RPM probe messages. This feature is supported only with <b>icmp-ping</b>, <b>icmp-ping-timestamp</b>, <b>udp-ping</b>, and <b>udp-ping-timestamp</b> probe types. You must also configure the <b>rpm</b> statement on the <b>sp-</b> interface and include the <b>unit 0 family inet</b> statement with a <b>/32</b> address.</p> <p>On M Series, MX Series, and T Series routers, specify a multiservices (<b>ms-</b>) interface that adds a timestamp to RPM probe messages. This feature is supported only with <b>icmp-ping</b>, <b>icmp-ping-timestamp</b>, <b>udp-ping</b>, and <b>udp-ping-timestamp</b> probe types. You must also configure the <b>rpm</b> statement on the <b>ms-</b> interface and include the <b>unit 0 family inet</b> statement with a <b>/32</b> address.</p> <p>To enable RPM for the extension-provider packages on the adaptive services interface, configure the <b>object-cache-size</b>, <b>policy-db-size</b>, and <b>package</b> statements at the [edit <b>chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider</b>] hierarchy level. For the extension-provider package, <b>package-name</b> in the <b>package package-name</b> statement is <b>jservices-rpm</b>.</p>
Options	<b>interface-name</b> —Name of the adaptive services interface.
Required Privilege Level	<b>system</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Configuring RPM Timestamping on page 1481</a></li><li>• <a href="#">Configuring RPM Receiver Servers on page 1480</a></li><li>• <a href="#">Configuring RPM Timestamping on page 1481</a></li><li>• <a href="#">hardware-timestamp on page 1531</a></li><li>• <a href="#">rpm</a></li><li>• <a href="#">Enabling RPM for the Junos OS extension-provider package on page 1486</a></li></ul>

## destination-port

---

<b>Syntax</b>	<code>destination-port <i>port</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm bgp], [edit <a href="#">services rpm probe owner test test-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	<p>Specify the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port to which a probe is sent. This statement is used only for TCP or UDP probe types.</p> <p>The value for the <b>destination-port</b> can be only 7 when you configure along with hardware timestamping. A constraint check prevents you for configuring any other value for the destination port in this case.</p> <p>This constraint does not apply when you are using one-way hardware timestamping along with <b>destination-port</b> and either <b>probe-type udp-ping</b> or <b>probe-type udp-ping-timestamp</b>.</p>
<b>Options</b>	<b>port</b> —The port number can be 7 or from 49,160 to 65,535.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li><li>• <a href="#">Configuring RPM Probes on page 1475</a></li></ul>

## destination-udp-port (RFC 2544 Benchmarking)

---

<b>Syntax</b>	<code>destination-udp-port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> <i>test-name</i> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X52 for ACX Series routers. Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.
<b>Description</b>	Specify the UDP port of the destination to be used in the UDP header for the generated frames. If you do not specify the UDP port, the default value of 4041 is used.
<b>Options</b>	<i>port-number</i> —UDP port number for the test frames <b>Default:</b> 4041
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li><li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li><li>• <a href="#">rfc2544-benchmarking on page 1544</a></li></ul>

## direction (RFC 2544 Benchmarking)

---

<b>Syntax</b>	<code>direction (egress   ingress);</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> <i>test-name</i> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X52 for ACX Series routers. Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.
<b>Description</b>	Specify the direction of the interface on which the test must be run. This parameter is valid only for a <b>ccc</b> family.
<b>Options</b>	<b>egress</b> —Causes the test to be run in the egress direction of the interface (network-to-network interface (NNI)).  <b>ingress</b> —Causes the test to be run in the ingress direction of the interface (user-to-network interface (UNI)).
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li><li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li><li>• <a href="#">rfc2544-benchmarking on page 1544</a></li></ul>

## dscp-code-point

<b>Syntax</b>	<code>dscp-code-point <i>dscp-bits</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the value of the Differentiated Services (DiffServ) field within the IP header. The DiffServ code point (DSCP) bits value must be set to a valid 6-bit pattern.
<b>Options</b>	<p><b><i>dscp-bits</i></b>—A valid 6-bit pattern; for example, 001111, or one of the following configured DSCP aliases:</p> <ul style="list-style-type: none"> <li>• <b>af11</b>—Default: 001010</li> <li>• <b>af12</b>—Default: 001100</li> <li>• <b>af13</b>—Default: 001110</li> <li>• <b>af21</b>—Default: 010010</li> <li>• <b>af22</b>—Default: 010100</li> <li>• <b>af23</b> —Default: 010110</li> <li>• <b>af31</b> —Default: 011010</li> <li>• <b>af32</b> —Default: 011100</li> <li>• <b>af33</b> —Default: 011110</li> <li>• <b>af41</b> —Default: 100010</li> <li>• <b>af42</b> —Default:100100</li> <li>• <b>af43</b> —Default:100110</li> <li>• <b>be</b>—Default: 000000</li> <li>• <b>cs1</b>—Default: 001000</li> <li>• <b>cs2</b>—Default: 010000</li> <li>• <b>cs3</b>—Default: 011000</li> <li>• <b>cs4</b>—Default: 100000</li> <li>• <b>cs5</b>—Default: 101000</li> <li>• <b>cs6</b>—Default: 110000</li> <li>• <b>cs7</b>—Default: 111000</li> <li>• <b>ef</b>—Default: 101110</li> <li>• <b>nc1</b>—Default: 110000</li> </ul>

- **nc2**—Default: 111000

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring RPM Probes on page 1475](#)

---

## family (RFC 2544 Benchmarking)

---

**Syntax** family (inet | ccc);

**Hierarchy Level** [edit [services](#) rpm [rfc2544-benchmarking](#) tests test-name test-name]

**Release Information** Statement introduced in Junos OS Release 12.3X52 for ACX Series routers.  
Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.

**Description** Configure the address type family for the benchmarking test.

**Options** **inet**—Indicates that the test is run on an IPv4 service.  
**ccc**—Indicates that the test is run on a circuit cross-connect (CCC) or Ethernet pseudowire service. The **direction** option specifies the direction (ingress or egress) to be used for the test.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring an RFC 2544-Based Benchmarking Test on page 1489](#)
- [RFC 2544-Based Benchmarking Tests Overview on page 1468](#)
- [rfc2544-benchmarking on page 1544](#)

## hardware-timestamp

<b>Syntax</b>	hardware-timestamp;
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> test-name]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.1. Statement applied to MX Series routers in Junos OS Release 10.0. Statement introduced in Junos OS Release 10.3 for EX Series switches.
<b>Description</b>	<p>On MX Series routers, on M-320 routers using the Enhanced Queuing MPC, and on EX Series switches only, enable timestamping of RPM probe messages in the Packet Forwarding Engine host processor. This feature is supported only with <b>icmp-ping</b>, <b>icmp-ping-timestamp</b>, <b>udp-ping</b>, and <b>udp-ping-timestamp</b> probe types.</p> <p>When you configure either <b>probe-type udp-ping</b> or <b>probe-type udp-ping-timestamp</b> along with the <b>hardware-timestamp</b> command, the value for the <b>destination-port</b> can be only 7. A constraint check prevents you for configuring any other value for the destination port in this case.</p> <p>This constraint does not apply when you are configuring <b>one-way-hardware-timestamp</b>.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring RPM Timestamping on page 1481</a></li> </ul>

## history-size

<b>Syntax</b>	history-size <i>size</i> ;
<b>Hierarchy Level</b>	[edit services rpm bgp], [edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> test-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the number of stored history entries.
<b>Options</b>	<p><b>size</b>—A value from 0 to 512.</p> <p><b>Default:</b> 50</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li> <li>• <a href="#">Configuring RPM Probes on page 1475</a></li> </ul>

## inactivity-timeout (Services RPM)

---

<b>Syntax</b>	<code>inactivity-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm twamp <a href="#">server</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Inactivity timeout period, in seconds.
<b>Options</b>	<b><i>seconds</i></b> —Length of time the session is inactive before it times out. <b>Default:</b> 1800 seconds
<b>Required Privilege Level</b>	<b>system</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## logical-system

---

<b>Syntax</b>	<code>logical-system <i>logical-system-name</i> {   [ <a href="#">routing-instances</a> <i>instance-name</i> ]; }</code>
<b>Hierarchy Level</b>	[edit services rpm bgp]
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6.
<b>Description</b>	Specify the logical system used by the probes.  The remaining statements are explained separately.
<b>Options</b>	<b><i>logical-system-name</i></b> —Logical system name.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li></ul>

## max-connection-duration

---

<b>Syntax</b>	<code>max-connection-duration <i>hours</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm twamp server]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	Specify the maximum time a connection can exist between a client and the server.
<b>Options</b>	<i>hours</i> —Number of hours a connection can exist between a client and the server.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## maximum-connections

---

<b>Syntax</b>	<code>maximum-connections <i>count</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm twamp server]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Maximum number of allowed connections between the server and all control client hosts.
<b>Options</b>	<i>count</i> —Maximum number of connections. <b>Range:</b> 1 through 1000 <b>Default:</b> 64
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## maximum-connections-per-client

---

<b>Syntax</b>	maximum-connections-per-client <i>count</i> ;
<b>Hierarchy Level</b>	[edit services rpm twamp server]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Maximum number of allowed connections between the server and a single control client host.
<b>Options</b>	<i>count</i> —Maximum number of connections. <b>Range:</b> 1 through 500 <b>Default:</b> 64
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## maximum-sessions

---

<b>Syntax</b>	maximum-sessions <i>count</i> ;
<b>Hierarchy Level</b>	[edit services rpm twamp server]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Maximum number of allowed test sessions the server can have running at one time.
<b>Options</b>	<i>count</i> —Maximum number of sessions. <b>Range:</b> 1 through 2048 <b>Default:</b> 64
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## maximum-sessions-per-connection

---

<b>Syntax</b>	<code>maximum-sessions-per-connection count;</code>
<b>Hierarchy Level</b>	[edit services rpm twamp server]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Maximum number of allowed sessions the server can open on a single client connection.
<b>Options</b>	<b>count</b> —Maximum number of sessions. <b>Default:</b> 64
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## mode (RFC 2544 Benchmarking)

---

<b>Syntax</b>	<code>mode reflect;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services rpm rfc2544-benchmarkingtests test-name test-name</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.
<b>Description</b>	Specify the test mode for the packets that are sent during the benchmarking test.
<b>Options</b>	<b>reflect</b> —Causes the test frames to be reflected on the chosen service (IPv4 or Ethernet).
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li><li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li><li>• <a href="#">rfc2544-benchmarking on page 1544</a></li></ul>

## moving-average-size

---

<b>Syntax</b>	<code>moving-average-size <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm bgp], [edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement Introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Enable statistical calculation operations to be performed across a configurable number of the most recent samples.
<b>Options</b>	<i>number</i> —Number of samples to be used in calculations. <b>Range:</b> 0 through 255
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring RPM Probes on page 1475</a></li></ul>

## one-way-hardware-timestamp

---

<b>Syntax</b>	<code>one-way-hardware-timestamp;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 9.3 for EX Series switches.
<b>Description</b>	Enable timestamping of RPM probe messages for one-way delay and jitter measurements. You must configure this statement along with the <b>destination-interface</b> statement to invoke timestamping. This feature is supported only with <b>icmp-ping</b> , <b>icmp-ping-timestamp</b> , <b>udp-ping</b> , and <b>udp-ping-timestamp</b> probe types.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring RPM Timestamping on page 1481</a></li><li>• <a href="#">destination-interface on page 1526</a></li><li>• <a href="#">hardware-timestamp on page 1531</a></li></ul>

## port

---

See the following sections:

- [port \(RPM\) on page 1537](#)
- [port \(TWAMP\) on page 1537](#)

### port (RPM)

<b>Syntax</b>	<code>port <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services rpm probe-server</a> ( <a href="#">tcp</a>   <a href="#">udp</a> )]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the port number for the probe server.
<b>Options</b>	<i>number</i> —Port number for the probe server. The value can be 7 or 49,160 through 65,535.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring RPM Receiver Servers on page 1480</a></li></ul>

### port (TWAMP)

<b>Syntax</b>	<code>port <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services rpm twamp server</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	TWAMP server listening port.
<b>Options</b>	<i>number</i> —Port number. <b>Range:</b> 1 through 65,535
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## probe

---

**Syntax**    `probe owner {  
              test test-name {  
                  data-fill data;  
                  data-size size;  
                  destination-interface interface-name;  
                  destination-port port;  
                  dscp-code-point dscp-bits;  
                  hardware-timestamp;  
                  history-size size;  
                  moving-average-size number;  
                  one-way-hardware-timestamp;  
                  probe-count count;  
                  probe-interval seconds;  
                  probe-type type;  
                  routing-instance instance-name;  
                  source-address address;  
                  target (url | address);  
                  test-interval interval;  
                  thresholds thresholds;  
                  traps traps;  
              }  
          }`

**Hierarchy Level**    [edit [services](#) rpm]

**Release Information**    Statement introduced before Junos OS Release 7.4.  
                              Statement introduced in Junos OS Release 9.3 for EX Series switches.

**Description**    Specify an owner name. The owner name combined with the test name represent a single RPM configuration instance.

**Options**    *owner*—Specify an owner name up to 32 characters in length.  
  
              The remaining statements are explained separately.

**Required Privilege Level**    system—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring RPM Probes on page 1475](#)

## probe-count

---

<b>Syntax</b>	<code>probe-count count;</code>
<b>Hierarchy Level</b>	<code>[edit services rpm bgp],</code> <code>[edit <a href="#">services rpm probe</a> owner <a href="#">test</a> test-name]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the number of probes within a test.
<b>Options</b>	<i>count</i> —A value from 1 through 15.
<b>Required Privilege Level</b>	<i>interface</i> —To view this statement in the configuration. <i>interface-control</i> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li><li>• <a href="#">Configuring RPM Probes on page 1475</a></li></ul>

## probe-interval

---

<b>Syntax</b>	<code>probe-interval interval;</code>
<b>Hierarchy Level</b>	<code>[edit services rpm bgp],</code> <code>[edit <a href="#">services rpm probe</a> owner <a href="#">test</a> test-name]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the time to wait between sending packets, in seconds.
<b>Options</b>	<i>interval</i> —Number of seconds, from 1 through 255.
<b>Required Privilege Level</b>	<i>interface</i> —To view this statement in the configuration. <i>interface-control</i> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li><li>• <a href="#">Configuring RPM Probes on page 1475</a></li></ul>

## probe-limit

---

<b>Syntax</b>	<code>probe-limit <i>limit</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Configure the maximum number of concurrent probes allowed.
<b>Options</b>	<b>limit</b> —Maximum number of concurrent probes allowed. <b>Range:</b> 1 through 500 (PTX Series Packet Transport Routers only) 1 through 200 <b>Default:</b> 100
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Limiting the Number of Concurrent RPM Probes on page 1481</a></li></ul>

## probe-server

```
Syntax  probe-server {
        tcp {
            destination-interface interface-name;
            port number;
        }
        udp {
            destination-interface interface-name;
            port number;
        }
    }
```

**Hierarchy Level** [edit [services](#) rpm]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.3 for EX Series switches.  
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

**Description** Specify the server to act as a receiver for the probes.  
  
The remaining statements are explained separately.



**NOTE:** The `destination-interface` statement is not supported on PTX Series routers.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring RPM Receiver Servers on page 1480](#)

## probe-type

---

<b>Syntax</b>	<code>probe-type type;</code>
<b>Hierarchy Level</b>	[edit services rpm bgp], [edit <a href="#">services rpm probe owner test test-name</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the packet and protocol contents of a probe.
<b>Options</b>	<b>type</b> —Specify one of the following probe type values: <ul style="list-style-type: none"><li>• <b>http-get</b>—(Not available at the [edit services rpm bgp] hierarchy level.) Sends a Hypertext Transfer Protocol (HTTP) get request to a target URL.</li><li>• <b>http-metadata-get</b>—(Not available at the [edit services rpm bgp] hierarchy level.) Sends an HTTP get request for metadata to a target URL.</li><li>• <b>icmp-ping</b>—Sends ICMP echo requests to a target address.</li><li>• <b>icmp-ping-timestamp</b>—Sends ICMP timestamp requests to a target address.</li><li>• <b>tcp-ping</b>—Sends TCP packets to a target.</li><li>• <b>udp-ping</b>—Sends UDP packets to a target.</li><li>• <b>udp-ping-timestamp</b>—Sends UDP timestamp requests to a target address.</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li></ul>

## routing-instance

---

<b>Syntax</b>	<code>routing-instance <i>instance-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> <i>test-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the routing instance used by the probes.
<b>Options</b>	<b><i>instance-name</i></b> —A routing instance configured at the <code>[edit routing-instance]</code> hierarchy level. <b>Default:</b> Internet routing table <code>inet.0</code> .
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring RPM Probes on page 1475</a></li></ul>

## routing-instances

---

<b>Syntax</b>	<code>routing-instances <i>instance-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services rpm bgp],</code> <code>[edit services rpm bgp logical-system <i>logical-system-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the routing instance used by the probes.
<b>Options</b>	<b><i>instance-name</i></b> —A routing instance configured at the <code>[edit routing-instances]</code> hierarchy level. <b>Default:</b> Internet routing table <code>inet.0</code> .
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li></ul>

## rfc2544-benchmarking

---

<b>Syntax</b>	<pre>rfc2544-benchmarking {   tests{     test-name (RFC 2544 Benchmarking) test-name {       test-interface interface-name;       mode reflect;       family (inet   ccc);       destination-ipv4-address address;       destination-udp-port port-number;       source-ipv4-address address;       source-udp-port port-number;       direction (egress   ingress);     }   } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X52 for ACX Series routers. Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.
<b>Description</b>	Configure the parameters for the RFC 2544-based benchmarking test. You must configure a test profile, which specifies the type of test and the manner in which it must be performed, and associate the test profile with a test name. The test name that you configure contains details, such as the address family and the test mode, for the test. You can associate the same test profile with multiple test names.
<b>Options</b>	<b>rfc2544-benchmarking</b> —Define the attributes for the RFC 2544-based benchmarking test to examine and analyze the performance characteristics of a network interconnecting device.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li><li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li><li>• <code>show services rpm rfc2544-benchmarking</code></li><li>• <code>show services rpm rfc2544-benchmarking test-id</code></li></ul>

## rpm

```

Syntax  rpm {
        bgp {
            data-fill data;
            data-size size;
            destination-port port;
            history-size size;
            logical-system logical-system-name <routing-instances routing-instance-name>;
            moving-average-size number;
            probe-count count;
            probe-interval seconds;
            probe-type type;
            routing-instances instance-name;
            test-interval interval;
        }
    }

```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure BGP neighbor discovery through RPM.

The remaining statements are explained separately.

**Usage Guidelines** See [“Configuring BGP Neighbor Discovery Through RPM” on page 1473](#).

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

## server

---

<b>Syntax</b>	<pre>server {   client-list <i>list-name</i> {     [ address <i>address</i> ];   }   inactivity-timeout <i>seconds</i>;   maximum-connections <i>count</i>;   maximum-connections-per-client <i>count</i>;   maximum-sessions <i>count</i>;   maximum-sessions-per-connection <i>count</i>;   port <i>number</i>; }</pre>
<b>Hierarchy Level</b>	[edit services rpm <a href="#">twamp</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	TWAMP server configuration settings.
<b>Options</b>	The remaining statements are described separately.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## server-inactivity-timeout

---

<b>Syntax</b>	<pre>server-inactivity-timeout <i>minutes</i>;</pre>
<b>Hierarchy Level</b>	[edit services rpm <a href="#">twamp server</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	The maximum time the Two-Way Active Measurement Protocol (TWAMP) server has to finish the TWAMP control protocol negotiation.
<b>Options</b>	<p><b>minutes</b>—Number of minutes the TWAMP server has to finish the TWAMP control protocol negotiation.</p> <p><b>Default:</b> 15 minutes</p> <p><b>Range:</b> 1-30 minutes</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring TWAMP on page 1484</a></li></ul>

## services (RPM)

---

<b>Syntax</b>	<code>services rpm { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Define the service rules to be applied to traffic.
<b>Options</b>	<code>rpm</code> —Identifies the RPM set of rules statements.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li><li>• <a href="#">Configuring RPM Probes on page 1475</a></li><li>• <a href="#">Configuring RPM Receiver Servers on page 1480</a></li><li>• <a href="#">Limiting the Number of Concurrent RPM Probes on page 1481</a></li><li>• <a href="#">Configuring RPM Timestamping on page 1481</a></li><li>• <a href="#">Configuring TWAMP on page 1484</a></li><li>• <a href="#">Enabling RPM for the Junos OS extension-provider package on page 1486</a></li></ul>

## source-address

---

<b>Syntax</b>	<code>source-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit <code>services rpm probe owner test test-name</code> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the source IP address used for probes. If the source IP address is not one of the router's or switch's assigned addresses, the packet will use the outgoing interface's address as its source.
<b>Options</b>	<code>address</code> —Valid IP address.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring RPM Probes on page 1475</a></li></ul>

## source-ipv4-address (RFC 2544 Benchmarking)

---

<b>Syntax</b>	<code>source-ipv4-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> <i>test-name</i> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X52 for ACX Series routers. Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.
<b>Description</b>	Specify the source IPv4 address to be used in generated test frames. This parameter is optional for both <b>ccc</b> and <b>inet</b> families. If you do not configure the source IPv4 address for an <b>inet</b> family, the source address of the interface is used to transmit the test frames.
<b>Options</b>	<b><i>address</i></b> —Valid IPv4 address. <b>Default:</b> If you do not configure the source IPv4 address for a <b>ccc</b> family, default value of 192.168.1.10 is used.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li><li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li><li>• <a href="#">rfc2544-benchmarking on page 1544</a></li></ul>

## source-udp-port (RFC 2544 Benchmarking)

---

<b>Syntax</b>	<code>source-udp-port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> <i>test-name</i> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.3X52 for ACX Series routers. Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.
<b>Description</b>	Specify the UDP port of the source to be used in the UDP header for the generated frames. If you do not specify the UDP port, the default value of 4041 is used.
<b>Options</b>	<b><i>port-number</i></b> —Source UDP port number for the test frames <b>Default:</b> 4041
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li><li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li><li>• <a href="#">rfc2544-benchmarking on page 1544</a></li></ul>

## target (Services RPM)

---

<b>Syntax</b>	<code>target (url <i>url</i>   address <i>address</i>);</code>
<b>Hierarchy Level</b>	<code>[edit services rpm probe <i>owner</i> test <i>test-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Packet Transport Routers.
<b>Description</b>	Specify the destination address or URL used for the probes.
<b>Options</b>	<b>url <i>url</i></b> —For HTTP probe types, specify a fully formed URL that includes <b>http://</b> in the URL address.  <b>address <i>address</i></b> —For all other probe types, specify an IPv4 address for the target host.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring RPM Probes on page 1475</a></li></ul>

## tcp

---

<b>Syntax</b>	<pre>tcp {   <b>destination-interface</b> <i>interface-name</i>;   <b>port</b> <i>port</i>; }</pre>
<b>Hierarchy Level</b>	<code>[edit <b>services</b> rpm <b>probe-server</b>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the port information for the TCP server.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring RPM Receiver Servers on page 1480</a></li></ul>

## test

---

**Syntax**    `test test-name {  
              data-fill data;  
              data-size size;  
              destination-interface interface-name;  
              destination-port port;  
              dscp-code-point dscp-bits;  
              hardware-timestamp;  
              history-size size;  
              moving-average-size number;  
              one-way-hardware-timestamp;  
              probe-count count;  
              probe-interval seconds;  
              probe-type type;  
              routing-instance instance-name;  
              source-address address;  
              target (url url | address address);  
              test-interval interval;  
              thresholds thresholds;  
              traps traps;  
          }`

**Hierarchy Level**    [edit [services](#) rpm [probe](#) owner]

**Release Information**    Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.3 for EX Series switches.  
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

**Description**    Specify the range of probes over which the standard deviation, average, and jitter are calculated. The test name combined with the owner name represent a single RPM configuration instance.

**Options**    **test-name**—Specify a test name. The name can be up to 32 characters in length.  
  
The remaining statements are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring RPM Probes on page 1475](#)

## tests (RFC 2544 Benchmarking)

**Syntax**

```
tests {
    test-name test-name {
        test-interface interface-name;
        mode reflect;
        family (inet | ccc);
        destination-ipv4-address address;
        destination-udp-port port-number;
        source-ipv4-address address;
        source-udp-port port-number;
        direction (egress | ingress);
    }
}
```

**Hierarchy Level** [edit [services](#) rpm [rfc2544-benchmarking](#)]

**Release Information** Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.

**Description** Specify the attributes of the test iteration, such as the address family (type of service, IPv4 or Ethernet), the logical interface, test duration, and test packet size, that are used for a benchmarking test to be run. The test name combined with the test profile represent a single real-time performance monitoring (RPM) configuration instance.

**Options** **tests**—Define the test iteration for the RFC 2544-based benchmarking test.

The remaining statements are explained separately.

**Required Privilege Level**

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring an RFC 2544-Based Benchmarking Test on page 1489](#)
- [RFC 2544-Based Benchmarking Tests Overview on page 1468](#)
- [rfc2544-benchmarking on page 1544](#)

## test-interface (RFC 2544 Benchmarking)

---

<b>Syntax</b>	<code>test-interface <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> <i>test-name</i> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.
<b>Description</b>	Specify the logical interface on which the RFC 2544-based benchmarking test is run. If you configure an <b>inet</b> family and the test mode to initiate and terminate test frames on the same device, the interface you configure is not effective. Instead, the test is run on the egress logical interface that is determined using route lookup on the specified destination IPv4 address. If you configure an <b>inet</b> family and the test mode to reflect the frames back on the sender from the other end, the logical interface is used as the interface to enable the reflection service (reflection is performed on the packets entering the specified interface). If you not configure the logical interface for reflection test mode, a lookup is performed on the source IPv4 address to determine the interface that hosts the address.
<b>Options</b>	<i>interface-name</i> —Name of the logical interface on which the test needs to be run.
<b>Required Privilege Level</b>	<i>interface</i> —To view this statement in the configuration. <i>interface-control</i> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li><li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li><li>• <a href="#">rfc2544-benchmarking on page 1544</a></li></ul>

## test-name (RFC 2544 Benchmarking)

---

<b>Syntax</b>	<pre>test-name <i>test-name</i> {     test-interface <i>interface-name</i>;     mode reflect;     family (inet   ccc);     destination-ipv4-address <i>address</i>;     destination-udp-port <i>port-number</i>;     source-ipv4-address <i>address</i>;     source-udp-port <i>port-number</i>;     direction (egress   ingress); }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarking</a> tests]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.
<b>Description</b>	Define the name of the RFC 2544-based benchmarking test. For each unique test name that you configure, you can specify a test profile, which contains the settings for a test and its type, and also a test interface, which contains the settings for test packets that are sent and received on the selected interface.
<b>Options</b>	<p><b>test-name</b>—Specify a test name. The name can be up to 32 characters in length.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 1489</a></li><li>• <a href="#">RFC 2544-Based Benchmarking Tests Overview on page 1468</a></li><li>• <a href="#">rfc2544-benchmarking on page 1544</a></li></ul>

## test-interval

---

<b>Syntax</b>	<code>test-interval <i>frequency</i>;</code>
<b>Hierarchy Level</b>	[edit services rpm bgp], [edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> <i>test-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Specify the time to wait between tests, in seconds.
<b>Options</b>	<i>frequency</i> —Number of seconds, from 0 through 86400.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring BGP Neighbor Discovery Through RPM on page 1473</a></li><li>• <a href="#">Configuring RPM Probes on page 1475</a></li></ul>

## traceoptions (RPM)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>; } </pre>
<b>Hierarchy Level</b>	[edit services rpm]
<b>Release Information</b>	Statement introduced in Junos OS Release 13.2.
<b>Description</b>	Define tracing operations for RPM processes.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. All files are placed in the directory <code>/var/log</code>.</p> <p><b>Default:</b> <code>rmopd</code></p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p><b>size <i>maximum-file-size</i></b>—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the <b>files</b> option.</p> <p><b>Range:</b> 10 KB through 1 GB</p> <p><b>Default:</b> 128 KB</p> <p><b>world-readable</b>—(Optional) Enable unrestricted file access.</p> <p><b>no-world-readable</b>—(Default) Disable unrestricted file access. This means the log file can be accessed only by the user who configured the tracing operation.</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all operations.</li> <li>• <b>configuration</b>—Trace configuration events.</li> <li>• <b>error</b>—Trace events related to catastrophic errors in daemon.</li> <li>• <b>ipc</b>—Trace IPC events.</li> <li>• <b>ppm</b>—Trace ppm events.</li> <li>• <b>statistics</b>—Trace statistics.</li> </ul>

**Required Privilege Level** trace—To view this statement in the configuration.  
trace-control—To add this statement to the configuration.

**Related Documentation**

- [Tracing RPM Operations on page 1487](#)

---

## thresholds

---

**Syntax** thresholds *thresholds*;

**Hierarchy Level** [edit [services](#) rpm [probe](#) owner [test](#) *test-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.3 for EX Series switches.  
Statement introduced in Junos OS Release 13.2 for PTX Packet Series Transport Routers.

**Description** Specify thresholds used for the probes. A system log message is generated when the configured threshold is exceeded. Likewise, an SNMP trap (if configured) is generated when a threshold is exceeded.

**Options** *thresholds*—Specify one or more threshold measurements. The following options are supported:

- **egress-time**—Measures maximum source-to-destination time per probe.
- **ingress-time**—Measures maximum destination-to-source time per probe.
- **jitter-egress**—Measures maximum source-to-destination jitter per test.
- **jitter-ingress**—Measures maximum destination-to-source jitter per test.
- **jitter-rtt**—Measures maximum jitter per test, from 0 through 60,000,000 microseconds.
- **rtt**—Measures maximum round-trip time per probe, in microseconds.
- **std-dev-egress**—Measures maximum source-to-destination standard deviation per test.
- **std-dev-ingress**—Measures maximum destination-to-source standard deviation per test.
- **std-dev-rtt**—Measures maximum standard deviation per test, in microseconds.
- **successive-loss**—Measures successive probe loss count, indicating probe failure.
- **total-loss**—Measures total probe loss count indicating test failure, from 0 through 15.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring RPM Probes on page 1475](#)

## traps

<b>Syntax</b>	<code>traps traps;</code>
<b>Hierarchy Level</b>	[edit <code>services rpm probe owner test test-name</code> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
<b>Description</b>	Set the trap bit to generate traps for probes. Traps are sent if the configured threshold is met or exceeded.
<b>Options</b>	<p><b>traps</b>—Specify one or more traps. The following options are supported:</p> <ul style="list-style-type: none"> <li>• <b>egress-jitter-exceeded</b>—Generates traps when the jitter in egress time threshold is met or exceeded.</li> <li>• <b>egress-std-dev-exceeded</b>—Generates traps when the egress time standard deviation threshold is met or exceeded.</li> <li>• <b>egress-time-exceeded</b>—Generates traps when the maximum egress time threshold is met or exceeded.</li> <li>• <b>ingress-jitter-exceeded</b>—Generates traps when the jitter in ingress time threshold is met or exceeded.</li> <li>• <b>ingress-std-dev-exceeded</b>—Generates traps when the ingress time standard deviation threshold is met or exceeded.</li> <li>• <b>ingress-time-exceeded</b>—Generates traps when the maximum ingress time threshold is met or exceeded.</li> <li>• <b>jitter-exceeded</b>—Generates traps when the jitter in round-trip time threshold is met or exceeded.</li> <li>• <b>probe-failure</b>—Generates traps for successive probe loss thresholds crossed.</li> <li>• <b>rtt-exceeded</b>—Generates traps when the maximum round-trip time threshold is met or exceeded.</li> <li>• <b>std-dev-exceeded</b>—Generates traps when the round-trip time standard deviation threshold is met or exceeded.</li> <li>• <b>test-completion</b>—Generates traps when a test is completed.</li> <li>• <b>test-failure</b>—Generates traps when the total probe loss threshold is met or exceeded.</li> </ul>



**NOTE:** For RPM traps to be generated, you must configure the `remote-operations SNMP` trap category by including the `categories` statement at the [edit `snmp trap-group trap-group-name`] hierarchy level.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring RPM Probes on page 1475](#)
- *categories*

---

## twamp

---

**Syntax**

```
twamp {  
  server {  
    authentication-mode mode;  
    client-list list-name {  
      [ address address ];  
    }  
    inactivity-timeout seconds;  
    max-connection-duration hours;  
    maximum-connections count;  
    maximum-connections-per-client count;  
    maximum-sessions count;  
    maximum-sessions-per-connection count;  
    port number;  
    server-inactivity-timeout minutes;  
  }  
}
```

**Hierarchy Level** [edit services rpm]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Two-Way Active Measurement Protocol (TWAMP) configuration settings.

The remaining statements are described separately.

**Required Privilege Level** system—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring TWAMP on page 1484](#)


## twamp-server

---

<b>Syntax</b>	twamp-server;
<b>Hierarchy Level</b>	[edit interfaces <i>sp-fpc/pic/port</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the service PIC logical interface to provide the TWAMP service.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring TWAMP on page 1484</a></li> </ul>

## udp

---

<b>Syntax</b>	<pre>udp {   destination-interface <i>interface-name</i>;   port <i>port</i>; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">services</a> rpm <a href="#">probe-server</a> ]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.</p>
<b>Description</b>	<p>Specify the port information for the UDP server.</p> <p>The remaining statements are explained separately.</p>
<div style="display: flex; align-items: center;">  <div> <p><b>NOTE:</b> The <code>destination-interface</code> statement is not supported on PTX Series routers.</p> </div> </div>	
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring RPM Receiver Servers on page 1480</a></li> </ul>



## PART 8

# Tunnel Services

- [Tunnel Services Overview on page 1563](#)
- [Tunnel Interfaces Configuration Guidelines on page 1567](#)
- [Summary of Tunnel Services Configuration Statements on page 1591](#)



# Tunnel Services Overview

This chapter discusses the following topics:

- [Tunnel Services Overview on page 1563](#)
- [GRE Keepalive Time Overview on page 1566](#)

## Tunnel Services Overview

---

By encapsulating arbitrary packets inside a transport protocol, tunneling provides a private, secure path through an otherwise public network. Tunnels connect discontinuous subnetworks and enable encryption interfaces, virtual private networks (VPNs), and MPLS. If you have a Tunnel Physical Interface Card (PIC) installed in your M Series or T Series router, you can configure unicast, multicast, and logical tunnels.

You can configure two types of tunnels for VPNs: one to facilitate routing table lookups and another to facilitate VPN routing and forwarding instance (VRF) table lookups.

For information about encryption interfaces, see [“Configuring Encryption Interfaces” on page 1101](#) and the *Junos OS Administration Library for Routing Devices*. For information about VPNs, see the *Junos OS VPNs Library for Routing Devices*. For information about MPLS, see the *Junos OS MPLS Applications Library for Routing Devices*.

On SRX Series and J Series devices, Generic Routing Encapsulation (GRE) and IP-IP tunnels use internal interfaces, `gr-0/0/0` and `ip-0/0/0`, respectively. The Junos OS creates these interfaces at system bootup; they are not associated with physical interfaces.

The Juniper Networks Junos OS supports the tunnel types shown in [Table 45 on page 1563](#).

**Table 45: Tunnel Interface Types**

Interface	Description
<code>gr-0/0/0</code>	<p>Configurable generic routing encapsulation (GRE) interface. GRE allows the encapsulation of one routing protocol over another routing protocol.</p> <p>Within a router, packets are routed to this internal interface, where they are first encapsulated with a GRE packet and then re-encapsulated with another protocol packet to complete the GRE. The GRE interface is an internal interface only and is not associated with a physical interface. You must configure the interface for it to perform GRE.</p>

Table 45: Tunnel Interface Types (*continued*)

Interface	Description
<b>gre</b>	<p>Internally generated GRE interface. This interface is generated by the Junos OS to handle GRE.</p> <p><b>NOTE:</b> You can configure GRE interfaces (gre-x/y/z) only for GMPLS control channels. GRE interfaces are not supported or configurable for other applications. This type of interface does not require a Tunnel PIC. For more information about GMPLS, see the <i>Junos OS MPLS Applications Library for Routing Devices</i> and the <i>Junos OS, Release 14.1</i>.</p>
<b>ip-0/0/0</b>	<p>Configurable IP-over-IP encapsulation (also called IP tunneling) interface. IP tunneling allows the encapsulation of one IP packet over another IP packet.</p> <p>Packets are routed to an internal interface where they are encapsulated with an IP packet and then forwarded to the encapsulating packet's destination address. The IP-IP interface is an internal interface only and is not associated with a physical interface. You must configure the interface for it to perform IP tunneling.</p>
<b>ipip</b>	Internally generated IP-over-IP interface. This interface is generated by the Junos OS to handle IP-over-IP encapsulation. It is not a configurable interface.
<b>lt-0/0/0</b>	<p>The <b>lt</b> interface on M Series and T Series routers supports configuration of logical systems—the capability to partition a single physical router into multiple logical devices that perform independent routing tasks.</p> <p>On SRX Series devices, the <b>lt</b> interface is a configurable logical tunnel interface that interconnects logical systems. See the <i>Junos OS Logical Systems Configuration Guide for Security Devices</i>.</p> <p>On J Series devices, the <b>lt</b> interface is used to provide class-of-service (CoS) support for real-time performance monitoring (RPM) probe packets. Packets are routed to this internal interface for services. The <b>lt</b> interface is an internal interface only; it is not associated with a physical interface. You must configure the interface for it to perform CoS for RPM services. See the <i>Junos OS Class of Service Configuration Guide for Security Devices</i>.</p>
<b>mt-0/0/0</b>	<p>Internally generated multicast tunnel interface. Multicast tunnels filter all unicast packets; if an incoming packet is not destined for a <b>224/8</b>-or-greater prefix, the packet is dropped and a counter is incremented.</p> <p>Within a router, packets are routed to this internal interface for multicast filtering. The multicast tunnel interface is an internal interface only and is not associated with a physical interface. If your router has a Tunnel Services PIC, the Junos OS automatically configures one multicast tunnel interface (<b>mt-</b>) for each virtual private network (VPN) you configure. You do not need to configure multicast tunnel interfaces. However, you can configure properties on <b>mt-</b> interfaces, such as the <b>multicast-only</b> statement.</p>
<b>mtun</b>	Internally generated multicast tunnel interface. This interface is generated by the Junos OS to handle multicast tunnel services. It is not a configurable interface.

Table 45: Tunnel Interface Types (*continued*)

Interface	Description
<b>pd-0/0/0</b>	<p>Configurable Protocol Independent Multicast (PIM) de-encapsulation interface. In PIM sparse mode, the first-hop router encapsulates packets destined for the rendezvous point router. The packets are encapsulated with a unicast header and are forwarded through a unicast tunnel to the rendezvous point. The rendezvous point then de-encapsulates the packets and transmits them through its multicast tree.</p> <p>Within a router, packets are routed to this internal interface for de-encapsulation. The PIM de-encapsulation interface is an internal interface only and is not associated with a physical interface. You must configure the interface for it to perform PIM de-encapsulation.</p> <p><b>NOTE:</b> On SRX Series devices, this interface type is <b>ppd0</b>.</p>
<b>pe-0/0/0</b>	<p>Configurable PIM encapsulation interface. In PIM sparse mode, the first-hop router encapsulates packets destined for the rendezvous point router. The packets are encapsulated with a unicast header and are forwarded through a unicast tunnel to the rendezvous point. The rendezvous point then de-encapsulates the packets and transmits them through its multicast tree.</p> <p>Within a router, packets are routed to this internal interface for encapsulation. The PIM encapsulation interface is an internal interface only and is not associated with a physical interface. You must configure the interface for it to perform PIM encapsulation.</p> <p><b>NOTE:</b> On SRX Series devices, this interface type is <b>ppe0</b>.</p>
<b>pimd</b>	Internally generated PIM de-encapsulation interface. This interface is generated by the Junos OS to handle PIM de-encapsulation. It is not a configurable interface.
<b>pime</b>	Internally generated PIM encapsulation interface. This interface is generated by the Junos OS to handle PIM encapsulation. It is not a configurable interface.
<b>vt-0/0/0</b>	<p>Configurable virtual loopback tunnel interface. Facilitates VRF table lookup based on MPLS labels. This interface type is supported on M Series and T Series routers, but not on SRX Series or J Series devices.</p> <p>To configure a virtual loopback tunnel to facilitate VRF table lookup based on MPLS labels, you specify a virtual loopback tunnel interface name and associate it with a routing instance that belongs to a particular routing table. The packet loops back through the virtual loopback tunnel for route lookup.</p>

#### Related Documentation

- [GRE Keepalive Time Overview on page 1566](#)
- [Configuring Unicast Tunnels on page 1567](#)
- [Restricting Tunnels to Multicast Traffic on page 1575](#)
- [Configuring Tunnel Interfaces on MX Series Routers on page 1582](#)
- [Configuring Tunnel Interfaces on T4000 Routers on page 1583](#)

## GRE Keepalive Time Overview

---

Generic routing encapsulation (GRE) tunnel interfaces do not have a built-in mechanism for detecting when a tunnel is down. You can enable keepalive messages to serve as the detection mechanism.

Keepalives can be configured on the physical or on the logical interface. If configured on the physical interface, keepalives are sent on all logical interfaces that are part of the physical interface. If configured on a individual logical interface, keepalives are only sent to that logical interface. In addition to configuring a keepalive, you must configure the hold time.

- Related Documentation**
- [Configuring GRE Keepalive Time on page 1573](#)
  - [keepalive-time on page 1598](#)
  - [hold-time \(OAM\) on page 1597](#)

# Tunnel Interfaces Configuration Guidelines

This chapter includes the following tunnel interface configuration tasks and examples:

- [Configuring Unicast Tunnels on page 1567](#)
- [Configuring GRE Keepalive Time on page 1573](#)
- [Restricting Tunnels to Multicast Traffic on page 1575](#)
- [Configuring Logical Tunnel Interfaces on page 1576](#)
- [Configuring Tunnel Interfaces for Routing Table Lookup on page 1577](#)
- [Configuring Virtual Loopback Tunnels for VRF Table Lookup on page 1578](#)
- [Configuring PIM Tunnels on page 1580](#)
- [Configuring IPv6-over-IPv4 Tunnels on page 1580](#)
- [Configuring IPv4-over-IPv6 Tunnels on page 1581](#)
- [Configuring Dynamic Tunnels on page 1581](#)
- [Configuring Tunnel Interfaces on MX Series Routers on page 1582](#)
- [Configuring Tunnel Interfaces on T4000 Routers on page 1583](#)
- [Examples: Configuring Unicast Tunnels on page 1584](#)
- [Example: Configuring a Virtual Loopback Tunnel for VRF Table Lookup on page 1586](#)
- [Example: Configuring an IPv6-over-IPv4 Tunnel on page 1586](#)
- [Example: Configuring an IPv4-over-IPv6 Tunnel on page 1587](#)
- [Example: Configuring Logical Tunnels on page 1589](#)

## Configuring Unicast Tunnels

---

To configure a unicast tunnel, you configure a **gr-** interface (to use GRE encapsulation) or an **ip-** interface (to use IP-IP encapsulation) and include the **tunnel** and **family** statements:

```
gr-fpc/pic/port or ip-fpc/pic/port {  
  unit logical-unit-number {  
    copy-tos-to-outer-ip-header;  
    reassemble-packets;  
    tunnel {  
      allow-fragmentation;  
      backup-destination address;  
    }  
  }  
}
```

```
destination destination-address;
do-not-fragment;
key number;
routing-instance {
    destination routing-instance-name;
}
source address;
ttl number;
}
family family {
    address address {
        destination address;
    }
}
}
```

You can configure these statements at the following hierarchy levels:

- [edit interfaces]
- [edit logical-systems *logical-system-name* interfaces]

You can configure multiple logical units for each GRE or IP-IP interface, and you can configure only one tunnel per unit.



**NOTE:** On M Series and T Series routers, you can configure the interface on a service PIC or a tunnel PIC. On MX Series routers, configure the interface on a Multiservices DPC.

---

Each tunnel interface must be a point-to-point interface. Point to point is the default interface connection type, so you do not need to include the **point-to-point** statement in the logical interface configuration.

You must specify the tunnel's destination and source addresses. The remaining statements are optional.



**NOTE:** For transit packets exiting the tunnel, forwarding path features, such as reverse path forwarding (RPF), forwarding table filtering, source class usage, destination class usage, and stateless firewall filtering, are not supported on the interfaces you configure as tunnel sources, but are supported on tunnel-pic interfaces.

However, class-of-service (CoS) information obtained from the GRE or IP-IP header is carried over the tunnel and is used by the re-entering packets. For more information, see the *Junos OS Class of Service Library for Routing Devices*.

To prevent an invalid configuration, the Junos OS disallows setting the address specified by the source or destination statement at the [edit interfaces *gr-fpc/pic/port* unit *logical-unit-number* tunnel] hierarchy level to be the same as the interface's own subnet address, specified by the address statement at the [edit interfaces *gr-fpc/pic/port* unit *logical-unit-number* family *family-name*] hierarchy level.

To set the time-to-live (TTL) field that is included in the encapsulating header, include the **ttl** statement. If you explicitly configure a TTL value for the tunnel, you must configure it to be one larger than the number of hops in the tunnel. For example, if the tunnel has seven hops, you must configure a TTL value of 8.

You must configure at least one family on the logical interface. To enable MPLS over GRE tunnel interfaces, you must include the **family mpls** statement in the GRE interface configuration. In addition, you must include the appropriate statements at the [edit **protocols**] hierarchy level to enable Resource Reservation Protocol (RSVP), MPLS, and label-switched paths (LSPs) over GRE tunnels. Unicast tunnels are bidirectional.

A configured tunnel cannot go through Network Address Translation (NAT) at any point along the way to the destination. For more information, see [“Examples: Configuring Unicast Tunnels” on page 1584](#) and the *Junos OS MPLS Applications Library for Routing Devices*.

For a GRE tunnel, the default is to set the ToS bits in the outer IP header to all zeros. To have the Routing Engine copy the ToS bits from the inner IP header to the outer, include the **copy-tos-bits-to-outer-ip-header** statement. (This inner-to-outer ToS bits copying is already the default behavior for IP-IP tunnels.)

For GRE tunnel interfaces on Adaptive Services or Multiservices interfaces, you can configure additional tunnel attributes, as described in the following sections:

- [Configuring a Key Number on GRE Tunnels on page 1570](#)
- [Enabling Fragmentation on GRE Tunnels on page 1570](#)
- [Specifying an MTU Setting for the Tunnel on page 1571](#)
- [Configuring a GRE Tunnel to Copy ToS Bits to the Outer IP Header on page 1571](#)
- [Configuring Packet Reassembly on page 1572](#)

## Configuring a Key Number on GRE Tunnels

For Adaptive Services and Multiservices interfaces on M Series and T Series routers, you can assign a key value to identify an individual traffic flow within a GRE tunnel, as defined in RFC 2890, *Key and Sequence Number Extensions to GRE*. However, only one key is allowed for each tunnel source and destination pair.

Each IP version 4 (IPv4) packet entering the tunnel is encapsulated with the GRE tunnel key value. Each IPv4 packet exiting the tunnel is verified by the GRE tunnel key value and de-encapsulated. The Adaptive Services or Multiservices PIC drops packets that do not match the configured key value.

To assign a key value to a GRE tunnel interface, include the **key** statement:

**key** *number*;

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* tunnel]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* tunnel]

The key number can be 0 through 4,294,967,295. You must configure the same GRE tunnel key value on tunnel endpoints.

The following example illustrates the use of the key statement in a GRE tunnel configuration:

```
interfaces {
  gr-1/2/0 {
    unit 0 {
      tunnel {
        source 10.58.255.193;
        destination 10.58.255.195;
        key 1234;
      }
      ...
      family inet {
        mtu 1500;
        address 10.200.0.1/30;
        ...
      }
    }
  }
}
```

## Enabling Fragmentation on GRE Tunnels

For GRE tunnel interfaces on Adaptive Services and Multiservices interfaces only, you can enable fragmentation of IPv4 packets in GRE tunnels.

By default, IPv4 traffic transmitted over GRE tunnels is not fragmented. To enable fragmentation of IPv4 packets in GRE tunnels, include the **clear-dont-fragment-bit** statement:

```
clear-dont-fragment-bit;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

When you include the **clear-dont-fragment-bit** statement in the configuration, the don't-fragment (DF) bit is cleared on all packets, even packets that do not exceed the tunnel maximum transmission unit (MTU). If the packet's size exceeds the tunnel's MTU value, the packet is fragmented before encapsulation. If the packet's size does not exceed the tunnel's MTU value, the packet is not fragmented.



**NOTE:** The Packet Forwarding Engine updates the IP identification field in the outer IP header of GRE-encapsulated packets, so that reassembly of the packets is possible after fragmentation. The previous CLI constraint check that required you to configure either the **clear-dont-fragment-bit** statement or a tunnel key with the **allow-fragmentation** statement is no longer enforced.

You can also clear the DF bit in packets transmitted over IP Security (IPsec) tunnels. For more information, see [“Enabling IPsec Packet Fragmentation” on page 509](#).

## Specifying an MTU Setting for the Tunnel

To enable key numbers and fragmentation on GRE tunnels (as described in [“Configuring a Key Number on GRE Tunnels” on page 1570](#) and [“Enabling Fragmentation on GRE Tunnels” on page 1570](#)), you must also specify an MTU setting for the tunnel.

To specify an MTU setting for the tunnel, include the **mtu** statement:

```
mtu bytes;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *gr-fpc/pic/port* unit *logical-unit-number* family inet]
- [edit logical-system *logical-system-name* interfaces *gr-fpc/pic/port* unit *logical-unit-number* family inet]

For more information about MTU settings, see the *Junos OS Network Interfaces Library for Routing Devices*.

## Configuring a GRE Tunnel to Copy ToS Bits to the Outer IP Header

Unlike IP-IP tunnels, GRE tunnels do not copy the ToS bits to the outer IP header by default. To have the Routing Engine copy the inner ToS bits to the outer IP header (which is required for some tunneled routing protocols) on packets sent by the Routing Engine,

include the **copy-tos-to-outer-ip-header** statement at the logical unit hierarchy level of a GRE interface. This example copies the inner ToS bits to the outer IP header on a GRE tunnel:

```
[edit interfaces]
gr-0/0/0 {
  unit 0 {
    copy-tos-to-outer-ip-header;
    family inet;
  }
}
```

## Configuring Packet Reassembly

On GRE tunnel interfaces only, you can enable reassembly of fragmented tunnel packets. To activate this capability, include the **reassemble-packets** statement:

```
reassemble-packets;
```

You can configure this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

For each tunnel you configure on the interface, you can enable or disable fragmentation of GRE packets by including the **allow-fragmentation** or **do-not-fragment** statement:

```
allow-fragmentation;
do-not-fragment;
```

You can configure these statements at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* tunnel]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* tunnel]

If you configure **allow-fragmentation** on a tunnel, it clears the DF bit in the outer IP header, enabling post fragmentation of GRE-encapsulated packets if the packet size exceeds the maximum transmission unit (MTU) value for the egress interface. By default, packets that exceed the MTU size are dropped and post fragmentation of GRE packets is disabled.



**NOTE:** Whenever you configure **allow-fragmentation** on a tunnel, you must also include either the **tunnel key** or the **clear-dont-fragment-bit** statement. This configuration enables the router to send affected packets to the PIC so that the correct IP header can be placed in the fragments. Otherwise, on the reassembly side some packets might be lost when fragments arrive in the PIC out of sequence at high speeds.

---

Related  
Documentation

- [Tunnel Services Overview on page 1563](#)

- [Examples: Configuring Unicast Tunnels on page 1584](#)

## Configuring GRE Keepalive Time

- [Configuring Keepalive Time and Hold time for a GRE Tunnel Interface on page 1573](#)
- [Display GRE Keepalive Time Configuration on page 1574](#)
- [Display Keepalive Time Information on a GRE Tunnel Interface on page 1574](#)

### Configuring Keepalive Time and Hold time for a GRE Tunnel Interface

You can configure the keepalives on a generic routing encapsulation (GRE) tunnel interface by including both the **keepalive-time** statement and the **hold-time** statement at the **[edit protocols oam gre-tunnel interface *interface-name*]** hierarchy level.



**NOTE:** For proper operation of keepalives on a GRE interface, you must also include the **family inet** statement at the **[edit interfaces *interface-name* unit *unit*]** hierarchy level. If you do not include this statement, the interface is marked as down.

To configure a GRE tunnel interface:

1. Configure the GRE tunnel interface at **[edit interfaces *interface-name* unit *unit-number*]** hierarchy level, where the interface name is gr-x/y/z, and the family is set as **inet**.  

```
user@host# set interfaces interface-name unit unit-number family family-name
```
2. Configure the rest of the GRE tunnel interface options as explained in *Configuring a GRE Tunnel Interface Between a PE and CE Router* or *Configuring a GRE Tunnel Interface Between PE Routers* based on requirement.

To configure keepalive time for a GRE tunnel interface:

- 1.
2. Configure the Operation, Administration, and Maintenance (OAM) protocol at the **[edit protocols]** hierarchy level for the GRE tunnel interface.  

```
[edit]
user@host# edit protocols oam
```
3. Configure the GRE tunnel interface option for OAM protocol.  

```
[edit protocols oam]
user@host# edit gre-tunnel interface interface-name
```
4. Configure the keepalive time from 1 through 50 seconds for the GRE tunnel interface.  

```
[edit protocols oam gre-tunnel interface interface-name]
user@host# set keepalive-time seconds
```
5. Configure the hold time from 5 through 250 seconds. Note that the hold time must be at least twice the keepalive time.  

```
[edit protocols oam gre-tunnel interface interface-name]
```

```
user@host# set hold-time (OAM) seconds
```

## Display GRE Keepalive Time Configuration

**Purpose** Display the configured keepalive time value as 10 and hold time value as 30 on a GRE tunnel interface (for example, gr-1/1/0.1):

**Action** To display the configured values on the GRE tunnel interface, run the **show oam gre-tunnel** command at the **[edit protocols]** hierarchy level:

```
[edit protocols]
user@host# show oam gre-tunnel
    interface gr-1/1/10.1 {
        keepalive-time 10;
        hold-time 30;
    }
```

## Display Keepalive Time Information on a GRE Tunnel Interface

<b>Purpose</b>	Display the current status information of a GRE tunnel interface when keepalive time and hold time parameters are configured on it and when the hold time expires.
----------------	--

**Action** To verify the current status information on a GRE tunnel interface (for example, gr-3/3/0.3), run the **show interfaces gr-3/3/0.3 terse** and **show interfaces gr-3/3/0.3 extensive** operational commands.

```
show interfaces gr-3/3/0.3 terse
```

```
user@host> show interfaces gr-3/3/0.3 terse
```

Interface	Admin	Link	Proto	Local	Remote
gr-3/3/0.3	up	up	inet mpls	200.1.3.1/24	

```
show interfaces gr-3/3/0.3 extensive
```

```
user@host> show interfaces gr-3/3/0.3 extensive
Logical interface gr-3/3/0.3 (Index 73) (SNMP ifIndex 594) (Generation 900)
Flags: Point-To-Point SNMP-Traps 0x4000 IP-Header
10.1.19.11:10.1.19.12:47:df:64:0000000000000000 Encapsulation: GRE-NULL
Gre keepalives configured: On, Gre keepalives adjacency state: down
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
Traffic statistics:
Input bytes :           15629992
Output bytes :          15912273
Input packets:            243813
Output packets:         179476
Local statistics:
Input bytes :           15322586
Output bytes :          15621359
Input packets:            238890
Output packets:         174767
Transit statistics:
Input bytes :             307406                0 bps
Output bytes :            290914                0 bps
Input packets:              4923               0 pps
Output packets:            4709               0 pps
```

```

Protocol inet, MTU: 1476, Generation: 1564, Route table: 0
Flags: Sendbroadcast-pkt-to-re
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
Destination: 200.1.3/24, Local: 200.1.3.1, Broadcast: 200.1.3.255,
Generation: 1366
Protocol mpls, MTU: 1464, Maximum labels: 3, Generation: 1565, Route table:
0

```

**NOTE:**

When the hold time expires:

- The GRE tunnel will stay up even though the interface cannot send or receive traffic.
- The Link status will be Up and the Gre keepalives adjacency state will be Down.

**Meaning** The current status information of a GRE tunnel interface with keepalive time and hold time parameters is displayed as expected when the hold time expires.

- Related Documentation**
- [GRE Keepalive Time Overview on page 1566](#)
  - [keepalive-time on page 1598](#)
  - [hold-time \(OAM\) on page 1597](#)

## Restricting Tunnels to Multicast Traffic

For interfaces that carry IPv4 or IP version 6 (IPv6) traffic, you can configure a tunnel interface to allow multicast traffic only. To configure a multicast-only tunnel, include the **multicast-only** statement:

```
multicast-only;
```

You can configure this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family *family*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *family*]

Multicast tunnels filter all unicast packets; if an incoming packet is not destined for a 224/8 or greater prefix, the packet is dropped and a counter is incremented.

You can configure this property on GRE, IP-IP, PIM, and multicast tunnel (**mt**) interfaces only.



**NOTE:** If your router has a Tunnel Services PIC, the Junos OS automatically configures one multicast tunnel interface (mt) for each virtual private network (VPN) you configure. You do not need to configure multicast tunnel interfaces.

**Related Documentation**

- [Tunnel Services Overview on page 1563](#)
- [Configuring Unicast Tunnels on page 1567](#)

## Configuring Logical Tunnel Interfaces

Logical tunnel (lt-) interfaces provide quite different services depending on the host router:

- On M Series, MX Series, and T Series routers, logical tunnel interfaces allow you to connect logical systems, virtual routers, or VPN instances. M Series and T Series routers must be equipped with a Tunnel Services PIC or an Adaptive Services Module (only available on M7i routers). MX Series routers must be equipped with a Trio MPC/MIC module. For more information about connecting these applications, see the *Junos OS VPNs Library for Routing Devices*.
- On SRX Series Services Gateways, the logical tunnel interface is used to interconnect logical systems. See the *Junos OS Logical Systems Configuration Guide for Security Devices*.
- On J Series Services Routers, the logical tunnel interface is used to provide class-of-service (CoS) support for real-time performance monitoring (RPM) probe packets. Packets are routed to this internal interface for services. See the *Junos OS Class of Service Configuration Guide for Security Devices*.

For M Series, MX Series, and T Series routers, see the following section:

- [Connecting Logical Systems on page 1576](#)

## Connecting Logical Systems

To connect two logical systems, you configure a logical tunnel interface on both logical systems. Then you configure a peer relationship between the logical tunnel interfaces, thus creating a point-to-point connection.

To configure a point-to-point connection between two logical systems, configure the logical tunnel interface by including the **lt-fpc/pic/port** statement:

```
lt-fpc/pic/port {
  unit logical-unit-number {
    encapsulation encapsulation;
    peer-unit unit-number; # peering logical system unit number
    dlcid dlcid-number;
    family (inet | inet6 | iso | mpls);
  }
}
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces]**
- **[edit logical-systems *logical-system-name* interfaces]**

When configuring logical tunnel interfaces, note the following:

- You can configure each logical tunnel interface with one of the following encapsulation types: Ethernet, Ethernet circuit cross-connect (CCC), Ethernet VPLS, Frame Relay, Frame Relay CCC, VLAN, VLAN CCC, or VLAN VPLS.
- You can configure the IP, IPv6, International Organization for Standardization (ISO), or MPLS protocol family.
- The peering logical interfaces must belong to the same logical tunnel interface derived from the Tunnel Services PIC or Adaptive Services Module.
- You can configure only one peer unit for each logical interface. For example, unit 0 cannot peer with both unit 1 and unit 2.
- To enable the logical tunnel interface, you must configure at least one physical interface statement.
- Logical tunnels are not supported with Adaptive Services, Multiservices, or Link Services PICs (but they are supported on the Adaptive Services Module on M7i routers, as noted above).
- On M Series routers other than the M40e router, logical tunnel interfaces require an Enhanced Flexible PIC Concentrator (FPC).
- On MX Series routers, logical tunnel interfaces require Trio MPC/MIC modules. They do not require a Tunnel Services PIC in the same system.

For more information about configuring logical systems, see the *Junos OS Routing Protocols Library for Routing Devices*.

#### Related Documentation

- [Tunnel Services Overview on page 1563](#)
- [Example: Configuring Logical Tunnels on page 1589](#)

## Configuring Tunnel Interfaces for Routing Table Lookup

To configure tunnel interfaces to facilitate routing table lookups for VPNs, you specify a tunnel's endpoint IP addresses and associate them with a routing instance that belongs to a particular routing table. This enables the Junos OS to search in the appropriate routing table for the route prefix, because the same prefix can appear in multiple routing tables. To configure the destination VPN, include the **routing-instance** statement:

```
routing-instance {
  destination routing-instance-name;
}
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *gr-fpc/pic/port* unit *logical-unit-number* tunnel]
- [edit logical-systems *logical-system-name* interfaces *gr-fpc/pic/port* unit *logical-unit-number* tunnel]

This configuration indicates that the tunnel's destination address is in routing instance *routing-instance-name*. By default, the tunnel route prefixes are assumed to be in the default Internet routing table **inet.0**.



**NOTE:** If you configure a virtual loopback tunnel interface and the **vrf-table-label** statement on the same routing instance, the **vrf-table-label** statement takes precedence over the virtual loopback tunnel interface. For more information, see “[Configuring Virtual Loopback Tunnels for VRF Table Lookup](#)” on page 1578.

For more information about VPNs, see the *Junos OS VPNs Library for Routing Devices*.

#### Related Documentation

- [Tunnel Services Overview](#) on page 1563
- [destination \(Routing Instance\)](#) on page 1593

## Configuring Virtual Loopback Tunnels for VRF Table Lookup

To enable egress filtering, you can either configure filtering based on the IP header, or you can configure a virtual loopback tunnel on routers equipped with a Tunnel PIC. [Table 46 on page 1578](#) describes each method.

**Table 46: Methods for Configuring Egress Filtering**

Method	Interface Type	Configuration Guidelines	Comments
Filter traffic based on the IP header	Nonchannelized Point-to-Point Protocol / High Level Data Link Control (PPP/HDLC) core-facing SONET/SDH interfaces	Include the <b>vrf-table-label</b> statement at the [edit <b>routing-instances</b> <i>instance-name</i> ] hierarchy level.  For more information, see the <i>Junos OS VPNs Library for Routing Devices</i> .	There is no restriction on customer-edge (CE) router-to-provider edge (PE) router interfaces.

Table 46: Methods for Configuring Egress Filtering (*continued*)

Method	Interface Type	Configuration Guidelines	Comments
Configure a virtual loopback tunnel on routers equipped with a Tunnel PIC	All interfaces	See the guidelines in this section.	<p>Router must be equipped with a Tunnel PIC.</p> <p>There is no restriction on the type of core-facing interface used or CE router-to-PE router interface used.</p> <p>You cannot configure a virtual loopback tunnel and the <b>vrf-table-label</b> statement at the same time.</p>

You can configure a virtual loopback tunnel to facilitate VRF table lookup based on MPLS labels. You might want to enable this functionality so you can do either of the following:

- Forward traffic on a PE router to CE device interface, in a shared medium, where the CE device is a Layer 2 switch without IP capabilities (for example, a metro Ethernet switch).

The first lookup is done based on the VPN label to determine which VRF table to refer to, and the second lookup is done on the IP header to determine how to forward packets to the correct end hosts on the shared medium.

- Perform egress filtering at the egress PE router.

The first lookup on the VPN label is done to determine which VRF table to refer to, and the second lookup is done on the IP header to determine how to filter and forward packets. You can enable this functionality by configuring output filters on the VRF interfaces.

To configure a virtual loopback tunnel to facilitate VRF table lookup based on MPLS labels, you specify a virtual loopback tunnel interface name and associate it with a routing instance that belongs to a particular routing table. The packet loops back through the virtual loopback tunnel for route lookup. To specify a virtual loopback tunnel interface name, you configure the virtual loopback tunnel interface at the **[edit interfaces]** hierarchy level and include the **family inet** and **family mpls** statements:

```
vt-fpc/pic/port {
  unit 0 {
    family inet;
    family mpls;
  }
  unit 1 {
    family inet;
  }
}
```

To associate the virtual loopback tunnel with a routing instance, include the virtual loopback tunnel interface name at the **[edit routing-instances]** hierarchy level:

```
interface vt-fpc/pic/port;
```



**NOTE:** On virtual loopback tunnel interfaces, none of the logical interface statements except the family statement is supported. Note that you can configure only `inet` and `mpls` families, and you cannot configure IPv4 or IPv6 addresses on virtual loopback tunnel interfaces. Also, virtual loopback tunnel interfaces do not support class-of-service (CoS) configurations.

**Related Documentation**

- [Tunnel Services Overview on page 1563](#)
- [Example: Configuring a Virtual Loopback Tunnel for VRF Table Lookup on page 1586](#)

---

## Configuring PIM Tunnels

PIM tunnels are enabled automatically on routers that have a tunnel PIC and on which you enable PIM sparse mode. You do not need to configure the tunnel interface.

PIM tunnels are unidirectional.

In PIM sparse mode, the first-hop router encapsulates packets destined for the rendezvous point (RP) router. The packets are encapsulated with a unicast header and are forwarded through a unicast tunnel to the RP. The RP then de-encapsulates the packets and transmits them through its multicast tree. To perform the encapsulation and de-encapsulation, the first-hop and RP routers must be equipped with Tunnel PICs.

The Junos OS creates two interfaces to handle PIM tunnels:

- **pe**—Encapsulates packets destined for the RP. This interface is present on the first-hop router.
- **pd**—De-encapsulates packets at the RP. This interface is present on the RP.



**NOTE:** The **pe** and **pd** interfaces do not support class-of-service (CoS) configurations.

**Related Documentation**

- [Tunnel Services Overview on page 1563](#)

---

## Configuring IPv6-over-IPv4 Tunnels

If you have a Tunnel PIC installed in your M Series or T Series router, you can configure IPv6-over-IPv4 tunnels. To define a tunnel, you configure a unicast tunnel across an existing IPv4 network infrastructure. IPv6/IPv4 packets are encapsulated in IPv4 headers and sent across the IPv4 infrastructure through the configured tunnel. You manually configure configured tunnels on each end point.

On SRX Series and J Series devices, Generic Routing Encapsulation (GRE) and IP-IP tunnels use internal interfaces, `gr-0/0/0` and `ip-0/0/0`, respectively. The Junos OS creates these interfaces at system bootup; they are not associated with a physical interface.

IPv6-over-IPv4 tunnels are defined in RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*. For information about configuring a unicast tunnel, see [“Configuring Unicast Tunnels” on page 1567](#). For an IPv6-over-IPv4 tunnel configuration example, see [“Example: Configuring an IPv6-over-IPv4 Tunnel” on page 1586](#).

**Related  
Documentation**

- [Tunnel Services Overview on page 1563](#)
- [Example: Configuring an IPv6-over-IPv4 Tunnel on page 1586](#)

## Configuring IPv4-over-IPv6 Tunnels

You can configure IPv6 IP-IP tunnels to carry IPv4 traffic across a network as specified in RFC 2473, *Generic Packet Tunneling in IPv6 Specification*. It is becoming common for networks to support IPv6 only. This feature provides a way to transition IPv4-based legacy networks to IPv6.

An IPv6 IP-IP tunnel is a virtual link between two IPv6 routers and is used to transmit data using IPv6 addressed packets. This feature allows you to encapsulate the IPv4 traffic into an IPv6 IP-IP tunnel across an IPv6 network. The tunnel is unidirectional and unicast addressed. For bi-directional connectivity, you need to configure a pair of unidirectional tunnels.

The following procedure outlines how to configure an IP-IP tunnel to carry IPv4 traffic between two IPv6 systems:

1. Configure the **family inet6** statement and the **family inet** statement at the **[edit interfaces *ip-interface-name* unit *number*]** hierarchy level.
2. Configure an IPv6 address for the **source** statement and the **destination** statement at the **[edit interfaces *ip-interface-name* tunnel]** hierarchy level.

**Related  
Documentation**

- [Example: Configuring an IPv4-over-IPv6 Tunnel on page 1587](#)

## Configuring Dynamic Tunnels

A VPN that travels through a non-MPLS network requires a GRE tunnel. This tunnel can be either a static tunnel or a dynamic tunnel. A static tunnel is configured manually between two PE routers. A dynamic tunnel is configured using BGP route resolution.

When a router receives a VPN route that resolves over a BGP next hop that does not have an MPLS path, a GRE tunnel can be created dynamically, allowing the VPN traffic to be forwarded to that route. Only GRE IPv4 tunnels are supported.

To configure a dynamic tunnel between two PE routers, include the **dynamic-tunnels** statement:

```
dynamic-tunnels tunnel-name {  
    destination-networks prefix;  
    source-address address;  
}
```

You can configure this statement at the following hierarchy levels:

- [edit routing-options]
- [edit routing-instances *routing-instance-name* routing-options]
- [edit logical-systems *logical-system-name* routing-options]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options]

For more information about configuring routing options or BGP, see the *Junos OS Routing Protocols Library for Routing Devices*. For more information about VPNs, see the *Junos OS VPNs Library for Routing Devices*.

- Related Documentation**
- [Tunnel Services Overview on page 1563](#)
  - [dynamic-tunnels on page 1596](#)

---

## Configuring Tunnel Interfaces on MX Series Routers

---

Because the MX Series routers do not support Tunnel Services PICs, you create tunnel interfaces on MX Series routers by including the following statements at the **[edit chassis]** hierarchy level:

```
[edit chassis]  
fpc slot-number {  
    pic number {  
        tunnel-services {  
            bandwidth (1g | 10g | 20g | 40g);  
        }  
    }  
}
```

**fpc slot-number** is the slot number of the DPC, MPC, or MIC. On the MX80 router, the range is 0 through 1. On other MX series routers, if two SCBs are installed, the range is 0 through 11. If three SCBs are installed, the range is 0 through 5 and 7 through 11.

The **pic number** On MX80 routers, if the FPC is 0, the PIC number can only be 0. If the FPC is 1, the PIC range is 0 through 3. For all other MX series routers, the range is 0 through 3.

**bandwidth (1g | 10g | 20g | 40g)** is the amount of bandwidth to reserve for tunnel traffic on each Packet Forwarding Engine.



**NOTE:** When you use MPCs and MICs, tunnel interfaces are soft interfaces and allow as much traffic as the forwarding-path allows, so it is advantageous to setup tunnel services without artificially limiting traffic by use of the `bandwidth` option. However, you *must* specify bandwidth when configuring tunnel services for MX Series routers with DPCs or FPCs. The GRE key option is not supported on the tunnel interfaces for DPCs on MX960 routers.

Bandwidth rates of 20 gigabits per second and 40 gigabits per second require use of an MX Series router with the 100-Gigabit Ethernet Modular Port Concentrator (MPC) and the 100-Gigabit CFP MIC.

**1g** indicates that 1 gigabit per second of bandwidth is reserved for tunnel traffic.

**10g** indicates that 10 gigabits per second of bandwidth is reserved for tunnel traffic.

**20g** indicates that 20 gigabits per second of bandwidth is reserved for tunnel traffic.

**40g** indicates that 40 gigabits per second of bandwidth is reserved for tunnel traffic.

If you specify a bandwidth that is not compatible, tunnel services are not activated. For example, you cannot specify a bandwidth of 1 Gbps for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC.

To verify that the tunnel interfaces have been created, issue the **show interfaces terse** operational mode command. For more information, see the [CLI Explorer](#). The bandwidth that you specify determines the port number of the tunnel interfaces that are created. When you specify a bandwidth of **1g**, the port number is always 10. When you specify any other bandwidth, the port number is always 0.



**NOTE:** Ingress queueing and tunnel services cannot be configured on the same MPC as it causes PFE forwarding to stop. Each feature can, however, be configured and used separately.

#### Related Documentation

- *Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC*
- *Example: Configuring Tunnel Interfaces on a 10-Gigabit Ethernet 4-Port DPC*
- *Example: Configuring Tunnel Interfaces on the MPC3E*
- *bandwidth (Tunnel Services)*
- *tunnel-services (Chassis)*
- *[edit chassis] Hierarchy Level*

## Configuring Tunnel Interfaces on T4000 Routers

To create tunnel interfaces on a T4000 Core Router, include the following statements at the **[edit chassis]** hierarchy level:

```
[edit chassis]
fpc slot-number {
  pic number {
    tunnel-services {
      bandwidth bandwidth-value;
    }
  }
}
```

**fpc slot-number** denotes the slot number of the FPC. On the T4000 router, the range is 0 through 7.



NOTE:

- This applies only to the T4000 Type 5 FPC. If any other type of FPC is configured in this slot, this configuration is ignored and no tunnel physical interface is created.
- When you use Type 5 FPCs, the tunnel interfaces are soft interfaces and allow as much traffic as the forwarding-path allows. So, it is advantageous to setup tunnel services without artificially limiting traffic by setting the **bandwidth** statement.

**pic number** on the T4000 router is 0 or 1.

**bandwidth bandwidth-value** is the amount of bandwidth to reserve for the tunnel traffic on each Packet Forwarding Engine. The bandwidth value accepted includes every multiple of 10g up to 100g.

If you specify a bandwidth that is not compatible, tunnel services are not activated. For example, you cannot specify a bandwidth of 1 Gbps for a Packet Forwarding Engine on a 100-Gigabit Ethernet PIC with CFP.

To verify that the tunnel interfaces have been created, issue the **show interfaces terse** operational mode command. For more information, see the *Junos Interfaces Command Reference*.

**Related  
Documentation**

- *bandwidth (Tunnel Services)*
- *tunnel-services (Chassis)*
- *[edit chassis] Hierarchy Level*

---

## Examples: Configuring Unicast Tunnels

Configure two unnumbered IP-IP tunnels:

```
[edit interfaces]
ip-0/3/0 {
  unit 0 {
    tunnel {
      source 192.168.4.18;
      destination 192.168.4.253;
```

```

    }
    family inet;
  }
  unit 1 {
    tunnel {
      source 192.168.4.18;
      destination 192.168.4.254;
    }
    family inet;
  }
}

```

Configure numbered tunnel interfaces by including an address at the **[edit interfaces ip-0/3/0 unit (0 | 1) family inet]** hierarchy level:

```

[edit interfaces]
ip-0/3/0 {
  unit 0 {
    tunnel {
      source 192.168.4.18;
      destination 192.168.4.253;
    }
    family inet {
      address 10.5.5.1/30;
    }
  }
  unit 1 {
    tunnel {
      source 192.168.4.18;
      destination 192.168.4.254;
    }
    family inet {
      address 10.6.6.100/30;
    }
  }
}

```

Configure an MPLS over GRE tunnel by including the **family mpls** statement at the **[edit interfaces gr-1/2/0 unit 0]** hierarchy level:

```

[edit interfaces]
gr-1/2/0 {
  unit 0 {
    tunnel {
      source 192.168.1.1;
      destination 192.168.1.2;
    }
    family inet {
      address 10.1.1.1/30;
    }
    family mpls;
  }
}

```

**Related Documentation**

- [Tunnel Services Overview on page 1563](#)
- [Configuring Unicast Tunnels on page 1567](#)

## Example: Configuring a Virtual Loopback Tunnel for VRF Table Lookup

---

Configure a virtual loopback tunnel for VRF table lookup:

```
[edit routing-instances]
routing-instance-1 {
  instance-type vrf;
  interface vt-1/0/0.0;
  interface so-0/2/2.0;
  route-distinguisher 2:3;
  vrf-import VPN-A-import;
  vrf-export VPN-A-export;
  routing-options {
    static {
      route 10.0.0.0/8 next-hop so-0/2/2.0;
    }
  }
}
routing-instance-2 {
  instance-type vrf;
  interface vt-1/0/0.1;
  interface so-0/3/2.0;
  route-distinguisher 4:5;
  vrf-import VPN-B-import;
  vrf-export VPN-B-export;
  routing-options {
    static {
      route 10.0.0.0/8 next-hop so-0/3/2.0;
    }
  }
}
[edit interfaces]
vt-1/0/0 {
  unit 0 {
    family inet;
    family mpls;
  }
  unit 1 {
    family inet;
  }
}
```

- Related Documentation**
- [Tunnel Services Overview on page 1563](#)
  - [Configuring Virtual Loopback Tunnels for VRF Table Lookup on page 1578](#)

## Example: Configuring an IPv6-over-IPv4 Tunnel

---

Configure a tunnel on both sides of the connection.

**Configuration on Router 1**

```
[edit]
interfaces {
  gr-1/0/0 {
    unit 0 {
```

```

    tunnel {
      source 10.19.2.1;
      destination 10.19.3.1;
    }
    family inet6 {
      address 2001:DB8:1:1/126;
    }
  }
}

```

#### Configuration on Router 2

```

[edit]
interfaces {
  gr-1/0/0 {
    unit 0 {
      tunnel {
        source 10.19.3.1;
        destination 10.19.2.1;
      }
      family inet6 {
        address 2001:DB8:2:1/126;
      }
    }
  }
}

```

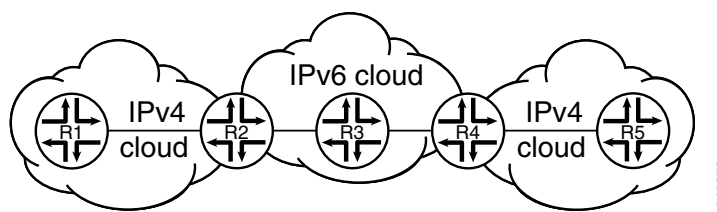
#### Related Documentation

- [Tunnel Services Overview on page 1563](#)
- [Configuring IPv6-over-IPv4 Tunnels on page 1580](#)

## Example: Configuring an IPv4-over-IPv6 Tunnel

You can configure IPv6 IP-IP tunnels to carry IPv4 traffic across a network as specified in RFC 2473, *Generic Packet Tunneling in IPv6 Specification*. It is becoming common for networks to support IPv6 only. This feature provides a way to transition IPv4-based legacy networks to IPv6.

**Figure 31: IPv6 Tunnel Connecting Two IPv4 Networks Across an IPv6 Network**



The following example is based on the topology shown in [Figure 31 on page 1587](#). Routers R2, R3, and R4 represent the IPv6 network. Routers R1 and R2 and R4 and R5 represent the IPv4 networks that need to be connected by an IPv6 tunnel. Routers R2 and R4 represent the IPv6 tunnel endpoints.

The following example illustrates the configuration for router R2 as shown in [Figure 31 on page 1587](#). On router R2, you configure an IPv4 over IPv6 uni-directional IP-IP tunnel which includes the following elements:

- The tunnel source IPv6 address is 2001:DB8:2::1. It could match Router R2's loopback address.
- The tunnel destination IPv6 address is 2001:DB8:3::1. It could match Router R4's loopback address.
- On Router R4, the tunnel receiving traffic from the Router R1 to R2 IPv4 network needs to have an IPv4 address in the same subnet as 1.1.1.1/30 (for example, 1.1.1.2).

```
[edit]
interfaces {
  ip-1/2/0 {
    unit 0 {
      tunnel {
        source 2001:DB8:2::1;
        destination 2001:DB8:3::1;
      }
      family inet {
        address 1.1.1.1/30;
      }
    }
  }
}
```

The output from the **show interfaces ip-1/2/0** command displays the following:

```
user@host> show interfaces ip-1/2/0
Physical interface: ip-1/2/0, Enabled, Physical link is Up
  Interface index: 144, SNMP ifIndex: 521
  Type: IPIP, Link-level type: IP-over-IP, MTU: Unlimited, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

Logical interface ip-1/2/0.0 (Index 74) (SNMP ifIndex 540)
  Flags: Point-To-Point SNMP-Traps 0x4000
  IP-Header 2001:db8:2::1-2001:db8:3::1-41-64-00000000
  Encapsulation: IPIP-NULL
  Input packets : 0
  Output packets: 0
  Protocol inet, MTU: Unlimited
    Flags: Sendbcst-pkt-to-re
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 1.1.1.0/30, Local: 1.1.1.1
```

```
astatti@tp9>
```

When attempting to configure an IPv4 over IPv6 tunnel, be aware of the following:

- The IP-IP interface comes up only when the tunnel source and tunnel destination reachability information is populated in the routing table.
- To carry IPv6 traffic over an IPv6 IP-IP tunnel, the IP interface needs to be configured with an IPv6 address (using **set interfaces *ip-interface-name* unit 0 family inet6 address *address***).

- Related Documentation**
- [Configuring IPv4-over-IPv6 Tunnels](#)
  - [Example: Configuring an IPv6-over-IPv4 Tunnel on page 1586](#)

## Example: Configuring Logical Tunnels

Configure three logical tunnels:

```
[edit interfaces]
lt-4/2/0 {
  description "Logical tunnel interface connects three logical systems";
}
[edit logical-systems]
lr1 {
  interfaces lt-4/2/0 {
    unit 12 {
      peer-unit 21; #Peering with lr2
      encapsulation frame-relay;
      dlci 612;
      family inet;
    }
    unit 13 {
      peer-unit 31; #Peering with lr3
      encapsulation frame-relay-ccc;
      dlci 613;
    }
  }
}
lr2 {
  interfaces lt-4/2/0 {
    unit 21 {
      peer-unit 12; #Peering with lr1
      encapsulation frame-relay-ccc;
      dlci 612;
    }
    unit 23 {
      peer-unit 32; #Peering with lr3
      encapsulation frame-relay;
      dlci 623;
    }
  }
}
lr3 {
  interfaces lt-4/2/0 {
    unit 31 {
      peer-unit 13; #Peering with lr1
      encapsulation frame-relay;
      dlci 613;
      family inet;
    }
    unit 32 {
      peer-unit 23; #Peering with lr2
      encapsulation frame-relay-ccc;
      dlci 623;
    }
  }
}
```

```
}  
}  
}
```

**Related  
Documentation**

- [Tunnel Services Overview on page 1563](#)
- [Configuring Logical Tunnel Interfaces on page 1576](#)

# Summary of Tunnel Services Configuration Statements

The following sections explain each of the tunnel services statements. The statements are organized alphabetically.

## allow-fragmentation

<b>Syntax</b>	allow-fragmentation;
<b>Hierarchy Level</b>	[edit interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> tunnel], [edit logical-systems <i>logical-system-name</i> interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> tunnel]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable fragmentation of generic routing encapsulation (GRE) encapsulated packets regardless of maximum transmission unit (MTU) value.
<b>Default</b>	By default, the GRE-encapsulated packets are dropped if the packet size exceeds the MTU setting of the egress interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">reassemble-packets on page 1600</a></li> <li>• <a href="#">Configuring Packet Reassembly on page 1572</a></li> </ul>

## backup-destination

---

<b>Syntax</b>	<code>backup-destination destination-address;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">unit logical-unit-number tunnel</a> ],[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <a href="#">unit logical-unit-number tunnel</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For tunnel interfaces, specify the remote address of the backup tunnel.
<b>Options</b>	<i>destination-address</i> —Address of the remote side of the connection.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">destination (Interfaces) on page 1113</a></li><li>• <a href="#">destination (Tunnel Remote End) on page 1223</a></li><li>• <a href="#">Configuring IPsec Tunnel Redundancy on page 1110</a></li></ul>

## copy-tos-to-outer-ip-header

---

<b>Syntax</b>	<code>copy-tos-to-outer-ip-header;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <i>unit logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <i>unit logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.2.
<b>Description</b>	For GRE tunnel interfaces only, enable the inner IP header's ToS bits to be copied to the outer IP packet header.
<b>Default</b>	If you omit this statement, the ToS bits in the outer IP header are set to 0.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring a GRE Tunnel to Copy ToS Bits to the Outer IP Header on page 1571</a></li></ul>

## destination

See the following sections:

- [destination \(Tunnel Remote End\) on page 1593](#)
- [destination \(Routing Instance\) on page 1593](#)

### destination (Tunnel Remote End)

<b>Syntax</b>	<code>destination <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
<b>Description</b>	For tunnel interfaces, specify the remote address of the tunnel.
<b>Options</b>	<b><i>destination-address</i></b> —Address of the remote side of the connection.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Unicast Tunnels on page 1567</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 1134</a></li> <li>• <a href="#">Configuring Flow Monitoring on page 1144</a></li> </ul>

### destination (Routing Instance)

<b>Syntax</b>	<code>destination <i>routing-instance-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> <i>routing-instance</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the destination routing instance that points to the routing table containing the tunnel destination address.
<b>Default</b>	The default Internet routing table <b>inet.0</b> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Tunnel Interfaces for Routing Table Lookup on page 1577</a></li> </ul>

## destination-networks

---

<b>Syntax</b>	<code>destination-networks <i>prefix</i>;</code>
<b>Hierarchy Level</b>	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> <a href="#">routing-options</a> dynamic-tunnels <i>tunnel-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> <a href="#">routing-options</a> dynamic-tunnels <i>tunnel-name</i> <i>rsvp-te entry</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> <a href="#">routing-options</a> dynamic-tunnels <i>tunnel-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> <a href="#">routing-options</a> dynamic-tunnels <i>tunnel-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> <a href="#">routing-options</a> dynamic-tunnels <i>tunnel-name</i> <i>rsvp-te entry</i>],</code> <code>[edit <a href="#">routing-options</a> dynamic-tunnels <i>tunnel-name</i>],</code> <code>[edit <a href="#">routing-options</a> dynamic-tunnels <i>tunnel-name</i> <i>rsvp-te entry</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.3 for ACX Series routers.
<b>Description</b>	Specify the IPv4 prefix range for the destination network. Only tunnels within the specified IPv4 prefix range can be created.
<b>Options</b>	<i>prefix</i> —Destination prefix of the network.
<b>Required Privilege Level</b>	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring GRE Tunnels for Layer 3 VPNs</a></li><li>• <a href="#">Configuring Dynamic Tunnels on page 1581</a></li><li>• <a href="#">Configuring RSVP Automatic Mesh</a></li></ul>

## do-not-fragment

---

<b>Syntax</b>	do-not-fragment;
<b>Hierarchy Level</b>	[edit interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> tunnel], [edit logical-systems <i>logical-system-name</i> interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> tunnel]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Set the do-not-fragment (DF) bit on the packets entering the GRE tunnel so that they do not get fragmented anywhere in the path.
<b>Default</b>	By default, fragmentation is disabled.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">reassemble-packets on page 1600</a></li><li>• <a href="#">Configuring Packet Reassembly on page 1572</a></li></ul>

## dynamic-tunnels

---

Syntax	<pre>dynamic-tunnels <i>tunnel-name</i> {   <i>destination-networks</i> <i>prefix</i>;   gre;   rsvp-te <i>entry-name</i> {     <i>destination-networks</i> <i>network-prefix</i>;     label-switched-path-template {       default-template;       <i>template-name</i>;     }   }   source-address <i>address</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> <a href="#">routing-options</a> ], [edit logical-systems <i>logical-system-name</i> <a href="#">routing-options</a> ], [edit routing-instances <i>routing-instance-name</i> <a href="#">routing-options</a> ], [edit <a href="#">routing-options</a> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure a dynamic tunnel between two PE routers.
Options	<b><i>tunnel-name</i></b> —Name of the dynamic tunnel.  The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <i>Example: Configuring a Two-Tiered Virtualized Data Center for Large Enterprise Networks</i></li><li>• <i>Configuring GRE Tunnels for Layer 3 VPNs</i></li><li>• See <a href="#">Configuring Dynamic Tunnels on page 1581</a>.</li></ul>

## hold-time (OAM)

---

<b>Syntax</b>	<code>hold-time seconds;</code>
<b>Hierarchy Level</b>	[edit protocols oam], [edit protocols oam gre-tunnel interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Length of time the originating end of a GRE tunnel waits for keepalive packets from the other end of the tunnel before marking the tunnel as operationally down.
<b>Options</b>	<b>seconds</b> —Hold-time value. <b>Default:</b> 5 seconds <b>Range:</b> 5 through 250 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">GRE Keepalive Time Overview on page 1566</a></li><li>• <a href="#">Configuring GRE Keepalive Time on page 1573</a></li><li>• <a href="#">keepalive-time on page 1598</a></li></ul>

## interfaces

---

<b>Syntax</b>	<code>interfaces { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure interfaces on the router.
<b>Default</b>	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Junos OS Network Interfaces Library for Routing Devices</a></li></ul>

## keepalive-time

---

<b>Syntax</b>	keepalive-time <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit protocols oam], [edit protocols oam gre-tunnel interface <i>interface-name</i> ], [edit protocols oam gre-tunnel interface <i>interface-name.unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Time difference between consecutive keepalive packets in a GRE tunnel.



**NOTE:** Support for GRE keepalive packets on MPC line cards became available as of Junos OS Release 11.4.

---

<b>Options</b>	<b><i>seconds</i></b> —Keepalive time value. <b>Default:</b> 1 second <b>Range:</b> 1 through 50 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">GRE Keepalive Time Overview on page 1566</a></li><li>• <a href="#">Configuring GRE Keepalive Time on page 1573</a></li><li>• <a href="#">hold-time (OAM) on page 1597</a></li></ul>

## key

<b>Syntax</b>	<code>key number;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Identify an individual traffic flow within a tunnel, as defined in RFC 2890, <i>Key and Sequence Number Extensions to GRE</i> . On M Series and T Series routers, you can configure the GRE interface on an Adaptive Services, Multiservices, or Tunnel PIC. On MX Series routers, configure the interface on a Multiservices DPC.
<b>Options</b>	<b>number</b> —Value of the key. <b>Range:</b> 0 through 4,294,967,295
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring a Key Number on GRE Tunnels on page 1570</a></li> </ul>

## multicast-only

<b>Syntax</b>	<code>multicast-only;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> <i>inet</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> <i>inet</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the unit and family so that the interface can transmit and receive multicast traffic only. You can configure this property on the IP family only.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Restricting Tunnels to Multicast Traffic on page 1575</a></li> <li>• <a href="#">tunnel on page 1604</a></li> </ul>

## peer-unit

---

<b>Syntax</b>	<code>peer-unit <i>unit-number</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure a peer relationship between two logical systems.
<b>Options</b>	<i>unit-number</i> —Peering logical system unit number.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Logical Tunnel Interfaces on page 1576</a></li></ul>

## reassemble-packets

---

<b>Syntax</b>	<code>reassemble-packets;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>gr-fpc/pic/port</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable reassembly of fragmented tunnel packets on generic routing encapsulation (GRE) tunnel interfaces.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Packet Reassembly on page 1572</a></li></ul>

## routing-instance

<b>Syntax</b>	routing-instance { <b>destination</b> <i>routing-instance-name</i> ; }
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the destination routing instance that points to the routing table containing the tunnel destination address.
<b>Default</b>	The default Internet routing table <b>inet.0</b> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Tunnel Interfaces for Routing Table Lookup on page 1577</a></li> </ul>

## routing-instances

<b>Syntax</b>	routing-instances <i>routing-instance-name</i> { ... }
<b>Hierarchy Level</b>	[edit], [edit logical-systems <i>logical-system-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure an additional routing entity for a router. You can create multiple instances of BGP, IS-IS, OSPF, OSPF version 3 (OSPFv3), and RIP for a router.
<b>Default</b>	Routing instances are disabled for the router.
<b>Options</b>	<b><i>routing-instance-name</i></b> —Name of the routing instance, a maximum of 31 characters. The remaining statements are explained separately.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring EVPN Routing Instances</a></li> <li>• <a href="#">Configuring Routing Instances on PE Routers in VPNs</a></li> </ul>

## routing-options

---

<b>Syntax</b>	routing-options { ... }
<b>Hierarchy Level</b>	[edit], [edit logical-systems <i>logical-system-name</i> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> ], [edit routing-instances <i>routing-instance-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure protocol-independent routing properties.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Protocol-Independent Routing Properties Feature Guide for Routing Devices</i></li></ul>

## source

---

<b>Syntax</b>	source <i>source-address</i> ;
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>tunnel</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX Series.
<b>Description</b>	Specify the source address of the tunnel.
<b>Default</b>	If you do not specify a source address, the tunnel uses the unit's primary address as the source address of the tunnel.
<b>Options</b>	<b><i>source-address</i></b> —Address of the local side of the tunnel. This is the address that is placed in the outer IP header's source field.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Configuring Generic Routing Encapsulation Tunneling (CLI Procedure)</i></li></ul>

## source-address

<b>Syntax</b>	<code>source-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> routing-options <b>dynamic-tunnels</b> <i>tunnel-name</i> ], [edit logical-systems <i>logical-system-name</i> routing-options <b>dynamic-tunnels</b> <i>tunnel-name</i> ], [edit routing-instances <i>routing-instance-name</i> routing-options <b>dynamic-tunnels</b> <i>tunnel-name</i> ], [edit routing-options <b>dynamic-tunnels</b> <i>tunnel-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.3 for ACX Series routers.
<b>Description</b>	Configure the tunnel source address.
<b>Options</b>	<b>address</b> —Name of the source address.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Dynamic Tunnels on page 1581</a></li> </ul>

## ttl

<b>Syntax</b>	<code>ttl <i>value</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>number</i> <b>tunnel</b> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
<b>Description</b>	Set the time-to-live value bit in the header of the outer IP packet.
<b>Options</b>	<b>value</b> —Time-to-live value. <b>Range:</b> 0 through 255 <b>Default:</b> 64
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Tunnel Properties</i></li> <li>• <i>Configuring Generic Routing Encapsulation Tunneling (CLI Procedure)</i></li> </ul>

## tunnel

---

<b>Syntax</b>	<pre>tunnel {   allow-fragmentation;   backup-destination address;   destination destination-address;   do-not-fragment;   key number;   routing-instance {     destination routing-instance-name;   }   source source-address;   ttl number; }</pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
<b>Description</b>	<p>Configure a tunnel. You can use the tunnel for unicast and multicast traffic or just for multicast traffic. You can also use tunnels for encrypted traffic or virtual private networks (VPNs).</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Encryption Interfaces on page 1101</a></li><li>• <i>Junos OS VPNs Library for Routing Devices</i></li></ul>

## unit (Interfaces)

<b>Syntax</b>	<pre> unit logical-unit-number {     peer-unit unit-number;     reassemble-packets;     tunnel {         allow-fragmentation;         backup-destination address;         destination destination-address;         do-not-fragment;         key number;         routing-instance {             destination routing-instance-name;         }         source source-address;         ttl number;     } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> interface-name], [edit logical-systems logical-system-name <a href="#">interfaces</a> interface-name]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
<b>Options</b>	<p><b>logical-unit-number</b>—Number of the logical unit.</p> <p><b>Range:</b> 0 through 16,384</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li> </ul>



## PART 9

# Index

- [Index on page 1609](#)
- [Index of Statements and Commands on page 1635](#)



# Index

## Symbols

#, comments in configuration statements.....	liv
( ), in syntax descriptions.....	liv
< >, in syntax descriptions.....	liv
[ ], in configuration statements.....	liv
{ }, in configuration statements.....	liv
(pipe), in syntax descriptions.....	liv

## A

AACL	
action statements.....	1060
applications.....	1059
best-effort application identification.....	988
example configuration.....	1064
logging flows.....	1061
match conditions.....	1059
rules.....	1062
aac-fields statement.....	1088
aac-statistics-profile statement.....	1089
accept	
action.....	1135
accounting statement	
flow monitoring.....	1216
usage guidelines.....	1202
acknowledge-retries statement.....	1442
usage guidelines.....	1399
acknowledge-timer statement.....	1443
usage guidelines.....	1399
action-red-differential-delay statement.....	1443
usage guidelines.....	1399
adaptive-services-pics statement.....	762
usage guidelines.....	1300
address statement	
APPID	
usage guidelines.....	997
application rule.....	1015
DFC.....	1349
usage guidelines.....	1330
encryption.....	1111
usage guidelines.....	1101

flow monitoring.....	1217
usage guidelines.....	1135
interfaces.....	814
usage guidelines.....	798
link services.....	1444
usage guidelines.....	1383
NAT.....	307
voice services.....	706
usage guidelines.....	696
address-allocation statement.....	307
address-range statement	
NAT.....	308
administrative statement	
BGF.....	847
aggregate-export-interval statement.....	1217
usage guidelines.....	1202
aggregation statement.....	457
flow monitoring.....	1218
usage guidelines.....	450, 1152
alert (system logging severity level).....	586, 755, 801
algorithm statement.....	849
ALGs	
application protocols.....	125
configuring.....	147
definition.....	125
ALGsJ	
default.....	62, 69
allow-fragmentation statement.....	1591
usage guidelines.....	1572
allow-ip-options statement.....	398
usage guidelines.....	390
allow-multicast statement.....	763
usage guidelines.....	756
allow-overlapping-nat-pools statement.....	308
allowed-destinations statement.....	1350
usage guidelines.....	1331
AMS	
HA.....	425, 426
NAT.....	425, 427
analyzer-address statement.....	1309
usage guidelines.....	1297
analyzer-id statement.....	1310
usage guidelines.....	1297
anomaly checklist.....	50
anti-replay-window-size statement.....	537, 764
usage guidelines.....	510, 750
any (system logging severity level).....	585, 755, 801
any-any match condition	
Ipsec.....	506

app-mapping-timeout statement.....	309	applications statement	
APPID		AACL.....	1067
best-effort application identification.....	988	usage guidelines.....	1059
example configuration.....	1010	APPID	
application layer gateways See ALGs		usage guidelines.....	1001
application protocol		application identification.....	1019
definition.....	125	application-level gateways.....	399
application statement.....	180, 1016, 1017	applications hierarchy.....	183
APPID		usage guidelines.....	125
usage guidelines.....	995	CoS.....	727
usage guidelines.....	146	usage guidelines.....	718
application-aware-access-list-fields		IDS.....	458
statement.....	1090	usage guidelines.....	449
application-data-inactivity-detection		NAT.....	310
statement.....	849	usage guidelines.....	205
application-group statement.....	1017	PTSP.....	957
APPID		stateful firewall.....	399
usage guidelines.....	1001	usage guidelines.....	389
application-group-any statement.....	1068	applying service set to interface.....	742
AACL		archive-sites statement.....	1310
usage guidelines.....	1059	usage guidelines.....	1299
PTSP.....	956	AS PIC	
application-groups statement.....	1018, 1068	multicast traffic.....	756
AACL		redundancy.....	589, 806, 1210
usage guidelines.....	1059	asymmetrical routing support	
APPID		APPID.....	1007
usage guidelines.....	1001	attack detection.....	445
PTSP.....	956	audit-observed-events-returns statement.....	850
application-profile statement.....	726	authentication statement.....	538
usage guidelines.....	720	usage guidelines.....	486
application-protocol statement.....	181	authentication-algorithm statement	
usage guidelines.....	147	IKE.....	539
application-set statement.....	182	usage guidelines.....	490
usage guidelines.....	163	IPsec.....	540
application-sets statement		usage guidelines.....	499
CoS.....	727	authentication-method statement.....	540
usage guidelines.....	718	usage guidelines.....	491
IDS.....	458	authentication-mode statement	
usage guidelines.....	449	RPM.....	1521
NAT.....	309	automatic statement.....	1019
usage guidelines.....	205	APPID	
stateful firewall.....	399	usage guidelines.....	1005
usage guidelines.....	389	autonomous-system-type statement.....	1219
application-system-cache-timeout		usage guidelines.....	1152
statement.....	1018	auxiliary-spi statement.....	541
APPID		usage guidelines.....	486
usage guidelines.....	1004		
applications.....	449	<b>B</b>	
example configuration.....	177	backup AS PIC.....	806

- backup Link Services IQ PIC.....621
- backup-destination statement.....1592
  - usage guidelines.....1110
- backup-interface statement.....1112
  - usage guidelines.....1109
- backup-remote-gateway statement.....541
  - usage guidelines.....509
- bandwidth
  - and delay buffer allocation.....638
  - guaranteed.....638, 643
- base-root statement.....851
- basic-nat-pt option
  - configuring.....240
- basic-nat44 option
  - configuring.....212
- basic-nat66 option
  - configuring.....217
- benchmarking test See RFC 2544 benchmarking
  - test, RPM service
- best-effort application identification.....988
- bfg-core statement.....852
- bgp statement
  - RPM.....1522
- braces, in configuration statements.....liv
- brackets
  - angle, in syntax descriptions.....liv
  - square, in configuration statements.....liv
- bundle statement.....706, 1444
  - usage guidelines.....700, 1383
- by-destination statement.....459
  - usage guidelines.....450
- by-pair statement.....460
  - usage guidelines.....450
- by-source statement.....461
  - usage guidelines.....450
- bypass-traffic-on-exceeding-flow-limits
  - statement.....765
- bypass-traffic-on-pic-failure statement.....765, 1020
  - usage guidelines.....742
- C**
- cancel-graceful statement.....854
- capture-group statement.....1351
  - usage guidelines.....1329
- cflowd statement.....1220
  - usage guidelines.....1152
- cgn-pic statement.....310, 815
  - NAT.....209
- CGNAT
  - ALGs.....62, 69
- chain-order statement
  - nested applications.....1020
- CIR.....643
- cisco-interoperability statement.....681
  - usage guidelines.....619
- cleanup-timeout statement.....855
- clear-dont-fragment-bit statement
  - GRE tunnel.....815
  - IPsec.....542
    - usage guidelines.....508
  - service-set.....766
    - usage guidelines.....509, 751, 802, 1570
- clear-ike-sas-on-pic-restart statement.....542
  - usage guidelines.....489
- clear-ipsec-sas-on-pic-restart statement.....543
  - usage guidelines.....489
- client-list statement.....1523
- close-timeout statement.....816
- collector statement.....1311
  - usage guidelines.....1298
- collector-pic statement
  - usage guidelines.....1300
- comments, in configuration statements.....liv
- compression statement.....707
  - usage guidelines.....697, 698
- compression-device statement.....707
  - usage guidelines.....700
- configuration
  - dynamic flow capture interface.....1335
  - flow collector interface.....1301
  - flow-tap application.....1346
- configuring NAT-PT with DNS application-level
  - gateways
    - example.....267
- content destinations
  - DFC.....1327
  - Junos Packet Vision.....1340
- content-destination statement.....1352
  - usage guidelines.....1330
- context statement
  - nested applications.....1021
- context-indications statement.....856
- control source
  - DFC.....1327
- control-association-indications statement.....857
- control-cores statement.....413

control-source statement.....	1353	default statement.....	860
usage guidelines.....	1331	delay buffer	
controller-address statement.....	858	calculating.....	638, 643
controller-failure statement.....	858	shaping rate.....	638, 643
controller-port statement.....	859	delay-buffer-rate statement	
conventions		usage guidelines.....	638
text and syntax.....	liii	delivery-function statement.....	861
copy-dont-fragment-bit statement		demux statement	
IPsec.....	543	PTSP.....	958
service-set.....	767	description statement	
usage guidelines.....	509	IKE.....	544
copy-tos-to-outer-ip-header statement.....	1592	usage guidelines.....	497
usage guidelines.....	1571	IPsec.....	544
core-dump statement.....	1222	usage guidelines.....	499, 502
usage guidelines.....	1144	destination NAT	
CoS		configuring.....	221, 251, 254
action statements.....	719	destination statement.....	415, 1113, 1445
applications.....	718	APPID	
example configuration.....	721	usage guidelines.....	997
for tunnels		application identification rule.....	1021
GRE TOS bits.....	1571	encryption	
link services interfaces.....	633, 636, 1401	usage guidelines.....	1101, 1110
link services IQ interfaces.....	615	flow monitoring	
match conditions.....	718	usage guidelines.....	1135
rules.....	722	link services	
scheduler map		usage guidelines.....	1383
configuration example.....	1395	tunnel.....	1593
count-type statement		usage guidelines.....	1567, 1577
PTSP.....	957	destination-address statement	
critical (system logging severity		AACL.....	1069
level).....	586, 755, 801	usage guidelines.....	1059
curly braces, in configuration statements.....	liv	BGF.....	861
customer support.....	lv	CoS.....	728
contacting JTAC.....	lv	usage guidelines.....	718
		IDS.....	462
		usage guidelines.....	449
<b>D</b>		IPsec.....	544
Data inactivity detection.....	923	usage guidelines.....	506
data session identification		NAT.....	311
APPID.....	999	usage guidelines.....	205
data statement.....	728	stateful firewall.....	400
usage guidelines.....	720	usage guidelines.....	389
data-cores statement.....	414	destination-address-range statement	
data-fill statement.....	1523	AACL.....	1069
data-flow-affinity statement.....	414	usage guidelines.....	1059
data-format statement.....	1311	IDS.....	462
usage guidelines.....	1298	usage guidelines.....	449
data-inactivity-detection statement.....	859		
data-size statement.....	1524		
dead peer detection (DPD) protocol.....	509		

NAT.....	312	system logging.....	1333
usage guidelines.....	205	threshold configuration.....	1334
stateful firewall.....	400	dh-group statement.....	545
usage guidelines.....	389	usage guidelines.....	491
destination-interface statement		dial-options statement.....	817
RPM.....	1526	interfaces	
destination-ipv4-address (RFC 2544		usage guidelines.....	587
Benchmarking).....	1525	diffserv statement.....	863
destination-networks statement		direction (RFC 2544 Benchmarking).....	1528
tunnel.....	1594	direction statement.....	546
usage guidelines.....	1581	nested applications.....	1022
destination-pool statement.....	312	usage guidelines.....	485
usage guidelines.....	206	disable statement	
destination-port range statement		APPID	
NAT.....	313	usage guidelines.....	995, 1001
destination-port statement		application.....	1023
applications.....	183	application group.....	1023
BGF.....	862	flow monitoring.....	1223
RPM.....	184, 1527	port mapping.....	1024
usage guidelines.....	152	traffic sampling	
destination-prefix statement.....	313, 463	usage guidelines.....	1137
usage guidelines.....	450	disable-all-instances statement	
destination-prefix-ipv6 statement.....	463	flow monitoring.....	1224
usage guidelines.....	450	disable-global-timeout-override statement.....	1024
destination-prefix-list statement		usage guidelines.....	995
ACL.....	1070	disable-mlppp-inner-ppp-pfc statement.....	1446
usage guidelines.....	1059	usage guidelines.....	1387
CoS.....	729	disable-session-mirroring statement.....	863
IDS.....	464	discard accounting	
NAT.....	314	usage guidelines.....	1202
stateful firewall.....	401	disconnect statement.....	864
usage guidelines.....	389	dlci statement.....	1446
destination-udp-port (RFC 2544		usage guidelines.....	1393
Benchmarking).....	1528	DLCIs	
destinations statement		multicast-capable connections.....	1393
flow collection.....	1312	point-to-point connections.....	1393
usage guidelines.....	1297	dnat-44 option	
destined-port statement		usage guidelines.....	221, 251, 254
NAT.....	314	do-not-fragment statement	
detect statement.....	862	tunnel.....	1595
deterministic-port-block-allocation		usage guidelines.....	1572
statement.....	315	documentation	
DFC		comments on.....	liv
architecture.....	1327	down statement.....	865
capture group.....	1329	download statement	
control source configuration.....	1331	APPID.....	1025
destination configuration.....	1330	usage guidelines.....	1005
example configuration.....	1335	drop-member-traffic statement	
interface configuration.....	1332	aggregated Multiservices.....	432

drop-timeout statement.....	1447	encapsulation statement.....	708
usage guidelines.....	1387	link services.....	1448
ds-lite statement.....	368	usage guidelines.....	1386
usage guidelines.....	343	voice services	
dscp statement.....	729	usage guidelines.....	699
BGF.....	866	encoding statement.....	866
usage guidelines.....	719	encrypted traffic identification	
dscp-code-point statement		APPID.....	1006
RPM.....	1529	encryption interface.....	1101
DTCP.....	1327, 1339	applying inbound filter.....	1107
duplicates-dropped-periodicity statement.....	1354	example configuration.....	1107
usage guidelines.....	1335	applying outbound filter.....	1106
dynamic address-only source translation		example configuration.....	1105, 1106
configuring.....	225	configuring inbound filter.....	1106
dynamic authentication.....	512	example configuration.....	1107
dynamic flow capture See DFC		configuring MTU.....	1102
dynamic NAT		encryption statement.....	548
configuring.....	225	usage guidelines.....	487
dynamic route insertion.....	513	encryption-algorithm statement	
dynamic rules.....	513	IKE.....	549
dynamic security associations		usage guidelines.....	492
usage guidelines.....	488, 489	IPsec.....	549
dynamic statement.....	547	usage guidelines.....	500
usage guidelines.....	488	engine-id statement	
Dynamic Tasking Control Protocol See DTCP		flow monitoring.....	1224
dynamic tunnels.....	1596	engine-type statement.....	1225
destination.....	1594	error (system logging severity level).....	586, 755, 801
source.....	1603	ES interfaces	
dynamic-flow-capture statement.....	1355	example configuration.....	1102
dynamic-nat44 option		ES PIC	
usage guidelines.....	225	apply inbound filter.....	1107
dynamic-tunnels statement.....	1596	PIC redundancy.....	1109
usage guidelines.....	1581	redundancy	
		example configuration.....	1109
<b>E</b>		tunnel redundancy.....	1110
ei-mapping-timeout statement.....	317	es-options statement.....	1114
emergency (system logging severity		usage guidelines.....	1109
level).....	585, 755, 801	event policy	
enable flow collection mode.....	1300	all (tracing flag).....	758
enable-asymmetric-traffic-processing		APPID.....	1009
statement.....	1026	configuration (tracing flag).....	758
enable-heuristics statement.....	1025, 1026	database (tracing flag).....	758
usage guidelines.....	1006	events (tracing flag).....	758
enable-rejoin statement		policy (tracing flag).....	758
aggregated Multiservices.....	433	event-timestamp-notification statement.....	867
		examples	
		configuring IP fragment reassembly on L2TP	
		LNS.....	590

- export-format statement.....1227
  - usage guidelines.....1146
- extension-provider statement.....416
- extension-service statement.....1226
- F**
  - f-max-period statement.....708
    - usage guidelines.....697
  - facility-override statement.....597, 768, 818
    - usage guidelines.....754
  - failover statement.....869
  - failover-cold statement.....867
  - failover-warm statement.....868
  - family (RFC 2544 Benchmarking).....1530
  - family statement
    - aggregated Multiservices.....433
    - encryption.....1115
      - usage guidelines.....1101
    - flow monitoring.....1228
      - usage guidelines.....1135
    - interfaces.....819
      - usage guidelines.....798
    - link services.....1450
      - usage guidelines.....1383
    - voice services.....709
  - fast-update-filters statement.....870
  - file statement.....1234
    - BGF.....871
    - L-PDF statistics.....1091
    - traffic sampling.....1233
    - traffic sampling output
      - usage guidelines.....1138, 1140
  - file-specification statement.....1313
    - usage guidelines.....1298
  - filename statement.....1234
  - filename-prefix statement.....1312
    - usage guidelines.....1299
  - files
    - logging information output file.....1140
    - traffic sampling output files.....1138
    - var/log/sampled file.....1140
    - var/tmp/sampled.pkts file.....1138
  - files statement.....1235
    - usage guidelines.....1138
  - filter statement
    - encryption.....1116
      - usage guidelines.....1107
    - flow monitoring.....1236
      - usage guidelines.....1135
  - filters
    - used with services.....742
  - firewall filters
    - actions.....1135
    - in traffic sampling.....1135
    - service filters.....804
  - flag statement.....872
  - flow aggregation.....1151
    - multiple flow servers.....1182
    - source ID, IPFIX flows.....1172
    - template and option template ID.....1167
    - traffic sampling
      - observation domain ID, version 9 .....1172
  - flow collector
    - analyzer configuration.....1297
    - destination configuration.....1297
    - example configuration.....1301
    - file format configuration.....1298
    - interface mapping.....1298
    - transfer log.....1299
  - flow limiting.....753
  - flow monitoring
    - example configuration
      - multiple port mirroring.....1192
      - next-hop groups.....1192
    - load balancing.....1199
    - overview.....1123
    - redundancy.....1210
  - Flow monitoring
    - overview.....1124, 1125
  - flow server
    - replicating flows to multiple servers.....1182
  - flow-active-timeout statement.....1237
    - usage guidelines.....1147
  - flow-collector statement.....1314
    - usage guidelines.....1295, 1300
  - flow-control-options statement.....1238
  - flow-export-destination statement.....1239
    - usage guidelines.....1146
  - flow-export-rate statement
    - flow monitoring.....1238
  - flow-inactive-timeout statement.....1240
    - usage guidelines.....1147
  - flow-monitoring statement.....1241
  - flow-server statement
    - flow monitoring.....1242
  - flow-tap
    - application.....1339
    - interface.....1342

permissions statement.....	1342	FRF.12.....	698
RADIUS configuration.....	1342	example configuration.....	668
restrictions.....	1343	LFI.....	1394
security.....	1342	LSQ.....	665
flow-tap application		FRF.15 and FRF.16.....	1375
example configuration.....	1346	FRF.16.....	655
flow-tap statement.....	1356	configuration example.....	658
flow-tap-dtcp statement.....	1342	from statement	
font conventions.....	liii	AACL.....	1070
force-entry statement.....	464	usage guidelines.....	1058
usage guidelines.....	450	CoS.....	730
forward-rule statement		usage guidelines.....	717
PTSP.....	960	HCM.....	1041
forwarding instance.....	959	usage guidelines.....	81
forwarding classes		IDS.....	465
fragmentation.....	633	usage guidelines.....	447, 449
forwarding-class statement.....	682, 730	IPsec.....	550
usage guidelines.....	633, 719	usage guidelines.....	504, 506
forwarding-db-size statement.....	417	NAT.....	318
setting for stateful firewall.....	411	usage guidelines.....	205
forwarding-options statement.....	1243	PTSP.....	961
usage guidelines.....	1130	PTSP forward rule.....	960
fragment reassembly		stateful firewall.....	402
configuring on L2TP LNS.....	590	usage guidelines.....	388, 389
on l2tp.....	589	ftp statement.....	731
fragment-threshold statement		flow collection.....	1316
link services.....	1451	usage guidelines.....	720, 1297, 1299
usage guidelines.....	1389	FTP traffic, sampling.....	1143
LSQ.....	683		
usage guidelines.....	633	<b>G</b>	
voice services.....	710	g-duplicates-dropped-periodicity statement.....	1357
usage guidelines.....	698	usage guidelines.....	1335
fragmentation		g-max-duplicates statement.....	1358
forwarding classes.....	633	usage guidelines.....	1335
GRE tunnels.....	1570	gateway statement	
multiclass MLPPP.....	636	BGF.....	873
fragmentation and reassembly.....	698, 1394	gateway-address statement.....	877
example configuration.....	1395	gateway-controller statement.....	878
fragmentation-map statement.....	683	gateway-port statement.....	879
usage guidelines.....	633	graceful statement.....	880
fragmentation-maps statement.....	684	graceful-restart statement.....	881
usage guidelines.....	633	GRE tunnels	
Frame Relay connections		fragmentation.....	1570
point-to-point connections.....	1393	key number.....	1570
Frame Relay encapsulation		guaranteed rate.....	643
multicast-capable connections.....	1393	guaranteed-rate statement	
		usage guidelines.....	643

## H

## H.248

properties	885, 903, 904, 905, 906, 907, 908, 909, 910, 913, 914
BFG	863
BGF	866
h248-options statement	882
h248-profile statement	884
h248-properties statement	885
h248-stack statement	888
h248-timers statement	889
hanging-termination-detection statement	889
hard-limit statement	1358
usage guidelines	1330
hard-limit-target statement	1359
usage guidelines	1330
hardware requirements	3
hardware-timestamp statement	1531
hash-key statement	418
hcm statement	1041
hello-interval statement	
L2TP	598
usage guidelines	584
hello-timer statement	
link services	1451
usage guidelines	1399
heuristics support	
APPID	1006
hide-avps statement	599
usage guidelines	585
high-availability-options statement	
aggregated Multiservices	434
history-size statement	1531
usage guidelines	1474
hold-time statement	
GRE tunnel interface	1597
host statement	769, 820
HCM	1042
L2TP	599
usage guidelines	585, 754, 801
hot-standby statement	685, 820

## I

icmp-code statement	185
usage guidelines	150
icmp-type statement	185
usage guidelines	150
icons defined, notice	lii

idle-timeout statement	1027
APPID	
usage guidelines	995
IDS	
action statements	450
applications	449
example configurations	454
match conditions	449
rules	447
ids-rule-sets statement	
usage guidelines	747
ids-rules statement	770
usage guidelines	747
ignore-entry statement	464
usage guidelines	450
ignore-errors statement	1027
usage guidelines	999
IKE	77, 489
authentication algorithm	
usage guidelines	490
authentication-method statement	
usage guidelines	491
DH (Diffie-Hellman) group	
usage guidelines	491
dynamic SAs	489
encryption-algorithm statement	
usage guidelines	492
lifetime	
usage guidelines	492
mode statement	
usage guidelines	495
policy	493
example	498
policy statement	
usage guidelines	493
pre-shared-key statement	
usage guidelines	495
proposals statement	
usage guidelines	495
version statement	
usage guidelines	494
IKE security associations	
clearing	489
ike statement	551
usage guidelines	489
ike-access-profile statement	770
usage guidelines	515, 750
inactivity-delay statement	890
inactivity-duration statement	890

inactivity-non-tcp-timeout statement.....	1028	interface-service statement.....	771
usage guidelines.....	995	usage guidelines.....	742
inactivity-tcp-timeout statement.....	1028	interfaces	
usage guidelines.....	995	naming.....	797
inactivity-timeout statement.....	186	interfaces statement	
BGF.....	891	aggregated Multiservices.....	435
flow monitoring.....	821	DFC.....	1360
RPM.....	1532	usage guidelines .....	1332
usage guidelines.....	155, 799	encryption.....	1116
inactivity-timer statement.....	892	usage guidelines.....	1101
index statement.....	1029	flow monitoring.....	1251
APPID		usage guidelines.....	1135
usage guidelines.....	995, 1001	interfaces hierarchy.....	822
nested applications.....	1029	usage guidelines.....	795
info (system logging severity level).....	586, 755, 802	link services.....	1452
initial-average-ack-delay statement.....	892	usage guidelines.....	1375
initiate-dead-peer-detection statement.....	552	tunnel.....	1597
usage guidelines.....	510	usage guidelines.....	1567
inline-jflow statement		voice services.....	710
flow monitoring.....	1243	interim-ah-scheme statement.....	893
usage guidelines.....	1176, 1181	interleave-fragments statement.....	1452
input statement		usage guidelines.....	1394
flow monitoring.....	1244	Internet Key Exchange See IKE	
interfaces.....	821	intrachassis LSQ failover.....	620
usage guidelines.....	742, 803	intrusion detection	
input-interface-index statement.....	1245	example configurations.....	454
input-packet-rate-threshold statement.....	1359	rule set.....	453
usage guidelines.....	1334	tasks.....	445
inside and outside interfaces.....	745	IP addresses	
inside-service-interface statement		sampling traffic from single IP addresses.....	1142
usage guidelines.....	746	IP fragment reassembly	
instance statement		configuring on L2TP LNS.....	590
port mirroring.....	1246	on l2tp.....	589
sampling.....	1247	ip statement	
usage guidelines.....	1175	APPID	
interchassis LSQ failover.....	618	usage guidelines.....	997
interface preservation.....	624	application identification.....	1030
interface statement		ip-flow-stop-detection statement.....	893
encryption		ip-reassembly statement	
usage guidelines.....	1101	L2TP LNS.....	600
flow monitoring.....	1249	ip-reassembly-rules statement	
usage guidelines.....	1187	service-set.....	771
flow-tap.....	1360	IPsec	
usage guidelines.....	1342	action statements.....	508
service interface pool.....	951	authentication statement	
interface style service sets.....	746	usage guidelines.....	486
interface-map statement.....	1318	authentication-algorithm statement	
usage guidelines.....	1298	usage guidelines.....	499

direction	
usage guidelines.....	485
dynamic authentication.....	512
dynamic endpoints interface	
configuration.....	516
dynamic rules.....	513
dynamic security associations	
usage guidelines.....	488
encryption	
usage guidelines.....	487
encryption-algorithm statement	
usage guidelines.....	500
ES PIC.....	1101
example configuration.....	520
inbound traffic.....	1107
outbound traffic.....	1105
IKE.....	77
lifetime of SA.....	500
lifetime-seconds statement.....	500
match conditions.....	506
minimum configurations	
dynamic SA .....	482
manual SA .....	481
overview.....	76
perfect-forward-secrecy statement	
usage guidelines.....	502
policy	
overview.....	501
policy statement	
usage guidelines.....	501
proposal statement	
usage guidelines.....	499
proposals statement	
usage guidelines.....	503
protocol statement (dynamic SA)	
usage guidelines.....	501
protocol statement (manual SA)	
usage guidelines.....	486
rule sets.....	511
security associations.....	76
security parameter index	
usage guidelines.....	486
service set dynamic endpoints	
configuration.....	515
traffic.....	1103
IPSec	
Services SDK	
configuration.....	519
ipsec statement.....	553
usage guidelines.....	499
ipsec-inside-interface	
usage guidelines.....	513
ipsec-inside-interface statement.....	553
usage guidelines.....	506
ipsec-interface-id statement	
usage guidelines.....	516
ipsec-sa statement	
encryption.....	1117
usage guidelines.....	1101
ipsec-transport-security-association	
statement.....	894
ipsec-vpn-options statement.....	772
usage guidelines.....	748
ipsec-vpn-rule-sets statement	
usage guidelines.....	747
ipsec-vpn-rules statement.....	772
usage guidelines.....	747
IPv4	
napt-44 option.....	229
translation type	
basic-nat-pt option.....	240
basic-nat44 option.....	212
basic-nat66 option.....	217
IPv4 dynamic source translation	
configuring.....	229
IPv4 static source translation	
AMS.....	427
example.....	427
ipv4-template statement.....	1251
IPv6	
napt-66 option.....	233
transition	
configured tunnel.....	1580
IPv6 dynamic source translation	
configuring.....	233
ipv6-multicast-interfaces statement.....	319
IPv6-over-IPv4 tunnel	
example configuration.....	1586
standards supported.....	1580
ipv6-template statement.....	1252
<b>J</b>	
jservices-sfw package.....	409
Junos Network Secure.....	48
overview.....	48
<i>See also</i> stateful firewall	

Junos Packet Vision		
architecture.....	1340	
<b>K</b>		
keepalive-time statement		
GRE tunnel interface.....	1598	
key statement		
tunnel.....	1599	
usage guidelines.....	1570	
<b>L</b>		
L-PDF		
best-effort application identification.....	988	
L2TP		
access profile.....	582, 583	
attribute-value pairs.....	585	
example configuration.....	593	
redundancy.....	589	
timers.....	584	
l2tp		
IP fragment reassembly overview.....	589	
l2tp statement		
usage guidelines.....	577	
L2TP statements		
LAC		
traceoptions.....	608	
LNS		
ip-reassembly (service sets).....	600	
ip-reassembly-rules.....	771	
l2tp-access-profile.....	600	
local-gateway.....	601	
service-interface.....	604	
traceoptions.....	608	
l2tp-access-profile statement.....	600	
usage guidelines.....	583	
l2tp-interface-id statement		
usage guidelines.....	587	
l2tp-profile statement		
usage guidelines.....	582	
label-position statement.....	1252	
latch-deadlock-delay statement.....	894	
lawful intercept architecture.....	1340	
learn-sip-register statement.....	186	
LFI.....	660, 665, 698, 1394	
example configuration.....	663, 668, 1395	
lifetime-seconds statement		
IKE.....	554	
usage guidelines.....	492	
IPsec.....	554	
usage guidelines.....	500	
limiting flows per service set.....	753	
link fragmentation and interleaving See LFI		
link PIC redundancy.....	624	
link services interface		
multilink bundles See multilink bundles		
link services interfaces		
CoS components.....	633, 636, 1401	
example configuration.....	1403, 1410	
interleave fragments.....	1394	
example configuration.....	1395	
link services IQ interfaces.....	663	
CoS components.....	615	
example configuration.....	652, 658	
link state replication.....	624	
link-layer overhead.....	635	
link services protocols.....	1371	
link state replication		
LSQ PICs.....	624	
link-layer overhead		
link services IQ interfaces.....	635	
link-layer-overhead statement.....	685	
usage guidelines.....	631, 635, 646	
lmi-type statement.....	1453	
usage guidelines.....	1400	
LNS (L2TP network server)		
configuring IP fragment reassembly.....	590	
load balancing		
on monitoring interfaces.....	1199	
load-balancing-options statement		
aggregated Multiservices.....	436	
local-address statement		
PTSP.....	962	
local-address-range statement		
PTSP.....	963	
local-certificate statement.....	554	
usage guidelines.....	496	
local-dump statement.....	1253	
usage guidelines.....	1185	
local-gateway address statement		
usage guidelines.....	583	
local-gateway statement.....	601, 773	
usage guidelines.....	748	
local-id statement.....	555	
usage guidelines.....	497	

local-policy-decision-function statement.....	1092	match-direction statement	
local-port-range statement		AACL.....	1071
PTSP.....	963	usage guidelines.....	1059
local-ports statement		CoS.....	731
PTSP.....	964	usage guidelines.....	718
local-prefix-list statement		IDS.....	466
PTSP.....	964	usage guidelines.....	447
log output		IPsec.....	556
adaptive services.....	757	usage guidelines.....	504
APPID.....	1009	NAT.....	320
traffic sampling.....	1140	PTSP.....	965
log-prefix statement.....	773, 822	stateful firewall.....	402
L2TP.....	601	usage guidelines.....	389
usage guidelines.....	585, 754, 801	max-burst-size statement.....	896
logging statement.....	466, 774	max-checked-bytes statement.....	1030
usage guidelines.....	450	APPID	
logical interface scheduling.....	690	usage guidelines.....	1004
logical interfaces		max-concurrent-calls statement.....	897
multicast-capable connections.....	1393	max-connection-duration statement.....	1533
logical tunnels.....	1576	max-duplicates statement.....	1361
example configuration.....	1589	usage guidelines.....	1335
logical-system statement		max-flows statement.....	775
RPM.....	1532	usage guidelines.....	753
usage guidelines.....	1474	max-packets-per-second statement.....	1255
loopback tunnels.....	1578	usage guidelines.....	1136
LSQ bandwidth		maximum-age statement.....	1319
oversubscribing.....	638	usage guidelines.....	1299
LSQ failover		maximum-connections statement.....	1533
interchassis.....	618	maximum-connections-per-client	
stateful intrachassis.....	621	statement.....	1534
stateless intrachassis.....	620	maximum-contexts statement.....	711
LSQ PICs.....	624	usage guidelines.....	697
redundancy.....	621	maximum-fuf-percentage statement.....	898
lsq-failure-options statement.....	686	maximum-inactivity-time statement.....	899
usage guidelines.....	618	maximum-net-propagation-delay statement.....	900
<b>M</b>		maximum-packet-length statement.....	1254
manual security association.....	484	maximum-send-window statement.....	602
manual statement.....	556	usage guidelines.....	584
usage guidelines.....	484	maximum-sessions statement.....	1534
manuals		maximum-sessions-per-connection	
comments on.....	liv	statement.....	1535
many-to-one statement		maximum-synchronization-mismatches	
aggregated Multiservices.....	437	statement.....	900
mapping-timeout statement.....	320	maximum-terms statement.....	901
match direction usage in service sets.....	745	maximum-transactions statement	
match statement.....	1253	nested applications.....	1031
		maximum-waiting-delay statement.....	901
		media statement.....	902

mediation devices	
Junos Packet Vision.....	1340
member statement	
nested applications.....	1031
member-failure-options statement	
aggregated Multiservices.....	438
member-interface statement	
aggregated Multiservices.....	440
mg-maximum-pdu-size statement.....	903
mg-originated-pending-limit statement.....	904
mg-provisional-response-timer-value	
statement.....	905
mg-segmentation-timer statement.....	906
mgc-maximum-pdu-size statement.....	907
mgc-originated-pending-limit statement.....	908
mgc-provisional-response-timer-value	
statement.....	909
mgc-segmentation-timer statement.....	910
min-checked-bytes statement.....	1032
APPID	
usage guidelines.....	1004
minimum links	
link services interfaces.....	1390
multilink interfaces.....	1390
minimum-links statement.....	1453
usage guidelines.....	1390
minimum-priority statement.....	1361
usage guidelines.....	1331
MLFR and MLPPP.....	1375
mlfr-uni-nni-bundle-options statement.....	1454
usage guidelines.....	1397, 1400
MLPPP.....	649, 660
configuration example.....	652
example configuration.....	663
MLPPP (Multilink Point-to-Point Protocol)	
sample topology.....	1421
mode (RFC 2544 Benchmarking).....	1535
mode statement.....	557
usage guidelines.....	495
monitor statement.....	911
monitoring statement.....	1256
usage guidelines.....	1145
moving-average-size statement.....	1536
MPLS	
packets	
passive flow monitoring.....	1205
mpls-ipv4-template statement.....	1257
mpls-template statement.....	1257
mrru statement.....	1455
usage guidelines.....	1391
MS-MPC	
configuration example	
napt.....	113, 263
mss statement.....	467
usage guidelines.....	450
mtu statement.....	1456
multicast traffic	
AS PIC.....	756
multicast tunnels.....	1575
multicast-capable connections	
Frame Relay encapsulation.....	1393
multicast-dlci statement.....	1456
usage guidelines.....	1393
multicast-only statement.....	1599
usage guidelines.....	1575
multiclass MLPPP	
fragmentation.....	636
multilink bundles	
fractional T1.....	660
example configuration.....	663, 665, 668
FRF.12.....	665
example configuration.....	668
MLPPP.....	660
example configuration.....	663
NxT1.....	649, 655
configuration example.....	652, 658
overview.....	1381
sample topology.....	1421
multilink interfaces	
example configuration.....	1406
minimum links.....	1390
multilink-class statement.....	686
usage guidelines.....	636
multilink-max-classes statement.....	687
usage guidelines.....	636
multiservice-options statement.....	1258
MultiServices PIC	
hardware requirements.....	40
<b>N</b>	
n391 statement.....	1457
usage guidelines.....	1400
n392 statement.....	1458
usage guidelines.....	1400
n393 statement.....	1459
usage guidelines.....	1400

- 
- name-format statement.....1320
    - usage guidelines.....1298
  - napt
    - configuration example.....113, 263
  - NAPT
    - comparison of implementation methods.....203
    - configuring.....229, 233
    - IPv4.....229
    - IPv6.....233
    - port allocation
      - round-robin.....195
      - sequential.....195
    - port block allocation.....198
  - napt-44 option
    - usage guidelines.....229
  - napt-66 option
    - usage guidelines.....233
  - napt-pt option
    - example.....267
  - NAT
    - action statements.....206
    - ALGs.....62, 69
    - AMS.....425
    - applications.....205
    - destination NAT.....221, 251
    - dynamic address-only source translation.....225
    - dynamic NAT.....225
    - dynamic source translation.....229, 233
    - inline.....59
      - configuring.....282
    - load balancing, example.....427
    - match conditions.....205
    - NAPT
      - configuring address pools.....194
    - NAT-PT example.....267
    - overview.....54
    - service sets.....209
    - session logging.....378
    - static destination address translation.....221, 251
    - twice NAT
      - description.....56
  - nat-options statement.....777
  - nat-rule-sets statement
    - usage guidelines.....747
  - nat-rules statement.....777
    - usage guidelines.....747
  - nested-application statement
    - APPID.....1033
    - usage guidelines.....1002
  - nested-application-settings statement
    - APPID.....1034
  - network address translation
    - configuration example
      - napt.....113, 263
  - network address translation See NAT
  - network-operator-id statement.....911
  - networks
    - sample LFI and multilink bundle
      - topology.....1421
    - sample multilink bundle and LFI
      - topology.....1421
  - next-hop groups.....1186
  - next-hop statement.....1258
    - next-hop groups
      - usage guidelines.....1187
    - usage guidelines.....1186
  - next-hop style service sets.....746
  - next-hop-group statement
    - forwarding-options.....1259
    - port mirroring.....1260
    - usage guidelines.....1186, 1187
  - next-hop-service statement.....778
    - usage guidelines.....744
  - no-anti-replay statement.....557, 779
    - usage guidelines.....510, 750
  - no-application-identification statement.....1034
    - APPID
      - usage guidelines.....1004
  - no-application-system-cache statement.....1035
    - APPID
      - usage guidelines.....1004
  - no-clear-application-system-cache
    - statement.....1035
    - APPID
      - usage guidelines.....1004
  - no-core-dump statement.....1222
    - usage guidelines.....1144
  - no-dscp-bit-mirroring statement.....912
  - no-filter-check statement.....1260
    - usage guidelines.....1186
  - no-fragmentation statement.....688
    - usage guidelines.....633
  - no-ipsec-tunnel-in-traceroute statement.....558
    - usage guidelines.....517
  - no-local-dump statement.....1253
    - usage guidelines.....1185
  - no-nested-application statement.....1036
    - usage guidelines.....1004

no-per-unit-scheduler statement.....	688
no-protocol-method statement.....	1036
APPID	
usage guidelines.....	1004
no-remote-trace statement	
flow monitoring.....	1261
no-rtcp-check statement.....	912
no-signature-based statement.....	1037
APPID	
usage guidelines.....	1004
no-stamp statement.....	1283
usage guidelines.....	1138
no-syslog statement	
DFC.....	1362
flow monitoring.....	1283
usage guidelines.....	1333
no-termination-request statement.....	689
usage guidelines.....	618
no-translation statement.....	321
usage guidelines.....	206
no-world-readable statement	
flow monitoring.....	1293
usage guidelines.....	1138
normal-mg-execution-time statement.....	913
normal-mgc-execution-time statement.....	914
notice (system logging severity level).....	586, 755, 801
notice icons defined.....	lii
Notification behavior.....	915
notification-behavior statement.....	915
notification-rate-limit statement.....	915
notification-regulation statement.....	916
notification-targets statement.....	1362
usage guidelines.....	1331
NxTl bundles	
FRF.16.....	655
configuration example.....	658
MLPPP.....	649
configuration example.....	652
<b>O</b>	
object-cache-size statement.....	419
setting for stateful firewall.....	411
observation-domain-id statement.....	1262
offloading flows	
configuring.....	808
one-way-hardware-timestamp statement.....	1536
usage guidelines.....	1482
open-timeout statement.....	823
usage guidelines.....	799
option-refresh-rate statement.....	1263
options-template-id statement.....	1264
order statement.....	1037
APPID	
usage guidelines.....	997
output files	
logging information output file.....	1140
traffic sampling output files.....	1138
output statement.....	824
discard accounting.....	1265
flow monitoring.....	1266
port mirroring.....	1267
sampling.....	1268
usage guidelines.....	742, 803
output-interface-index statement.....	1269
outside-service-interface statement	
usage guidelines.....	746
overload-control statement.....	916
overload-pool statement.....	321
usage guidelines.....	206
overload-prefix statement.....	322
usage guidelines.....	206
oversubscription.....	638
<b>P</b>	
package statement	
loading on PIC.....	420
packages	
jservices-sfw.....	409
packet-based IPsec.....	506
parentheses, in syntax descriptions.....	liv
passive flow monitoring.....	1124, 1125
MPLS packets.....	1205
passive-mode-tunneling statement.....	780
usage guidelines.....	752
passive-monitor-mode statement.....	1270
usage guidelines.....	1203
password statement	
flow collection.....	1322
usage guidelines.....	1297, 1299
pattern statement	
nested applications.....	1038
peak-data-rate statement.....	917, 918
peer-unit statement	
tunnel.....	1600
usage guidelines.....	1576
per-unit scheduling.....	690

per-unit-scheduler statement.....	690	port mirroring.....	1186
usage guidelines.....	638, 643, 649, 655	disabling.....	1223
perfect-forward-secrecy statement.....	558	disabling all instances.....	1224
usage guidelines.....	502	port statement	
pgcp-rules statement		cflowd	
service-set.....	780	usage guidelines.....	1152
PIC types for services.....	3	flow monitoring.....	1272
pic-memory-threshold statement.....	1363	NAT.....	324
usage guidelines.....	1334	RPM.....	1537
PIM		TWAMP.....	1537
tunnels.....	1580	voice services.....	712
PIR.....	638	usage guidelines.....	697
platform statement.....	919	port-forwarding	
platforms, supported.....	5	example.....	255
point-to-point connections		port-forwarding statement	
Frame Relay encapsulation.....	1393	destined-port statement.....	314
policy statement		NAT.....	325
IKE.....	559	translated-port statement.....	337
usage guidelines.....	493	port-forwarding-mappings statement.....	325
IPsec.....	560	port-mapping statement.....	1038
usage guidelines.....	501	port-mirroring statement.....	1273
policy-db-size statement.....	421	usage guidelines.....	1186
setting for stateful firewall.....	411	port-range statement.....	1039
policy-decision-statistics-profile statement.....	1093	APPID	
pool statement.....	323	usage guidelines.....	997
service interface pool.....	952	ports-per-session statement.....	326
pop-all-labels statement.....	1271	post-service-filter statement.....	824
usage guidelines.....	1205	usage guidelines.....	742
port block allocation.....	198	ppp-access-profile statement.....	602
deterministic.....	199	usage guidelines.....	583
algorithms.....	199	ppp-profile statement	
configuring.....	237	usage guidelines.....	582
interim syslog messages.....	378	pre-rewrite-tos statement	
secured.....	198, 199	usage guidelines.....	1137
configuring.....	235	pre-shared-key statement.....	560
Port Control Protocol		usage guidelines.....	495
Configuring.....	257	preserve-interface statement.....	691
Configuring a Service Set to Apply PCP.....	259	usage guidelines.....	624
Configuring PCP Server Options.....	257, 258	primary statement	
port forwarding		link services.....	691
configuring.....	254	usage guidelines.....	621
dnat-44.....	251	services PIC.....	825
static destination address translation.....	251	usage guidelines.....	806
without destination address translation.....	254	probe statement	
port forwarding without static destination address		RPM.....	1538
translation		probe-count statement.....	1539
configuring.....	254	probe-interval statement.....	1539
		probe-limit statement.....	1540
		probe-server statement.....	1541

probe-type statement.....	1542
procedural overview.....	46
profile statement	
APPID	
usage guidelines.....	1001
application identification.....	1039
profile-name statement.....	920
profile-version statement.....	920
proposal statement	
IKE.....	561
usage guidelines.....	489
IPsec.....	562
usage guidelines.....	499
proposals statement	
IKE.....	562
usage guidelines.....	495
IPsec.....	562
usage guidelines.....	503
protocol statement	
applications.....	187
usage guidelines.....	149
IPsec.....	563
usage guidelines.....	486, 501
nested applications.....	1040
PTSP.....	965
PTSP statements	
application-group-any.....	956
application-groups.....	956
applications.....	957
count-type.....	957
demux.....	958
forward-rule	
.....	960
forwarding instance.....	959
local-address.....	962
local-address-range.....	963
local-port-range.....	963
local-ports.....	964
local-prefix-list.....	964
match-direction.....	965
protocol.....	965
remote-address.....	966
remote-address-range.....	967
remote-port-range.....	967
remote-ports.....	968
remote-prefix-list.....	968
rule-set.....	970
services.....	971
term	
forward rule.....	972
rule.....	973
then	
forward rule.....	974
rule.....	975
ptsp-rule-sets statement	
usage guidelines.....	747
ptsp-rules statement.....	781
usage guidelines.....	747
<b>Q</b>	
queue-limit-percentage statement.....	921
queues statement.....	712
usage guidelines.....	697
<b>R</b>	
RADIUS servers	
configuration example.....	427
random-allocation statement.....	324
rate statement.....	825, 1274
usage guidelines.....	1136, 1186
reassemble-packets statement.....	1600
usage guidelines.....	1572
receive-options-packets statement.....	1274
usage guidelines.....	1203
receive-ttl-exceeded statement.....	1275
usage guidelines.....	1203
receive-window statement.....	603
usage guidelines.....	584
reconnect statement.....	922
red-differential-delay statement.....	1459
usage guidelines.....	1399
redistribute-all-traffic statement	
aggregated Multiservices.....	441
redundancy	
AS PIC.....	806
flow monitoring.....	1210
L2TP.....	589
redundancy-options statement.....	692, 826
usage guidelines.....	806
reflexive   reverse statement.....	732
usage guidelines.....	721
reject-all-commands-threshold statement.....	922
reject-new-calls-threshold statement.....	923
rejoin-timeout statement	
aggregated Multiservices.....	442
remote-address statement	
PTSP.....	966

remote-address-range statement		
PTSP.....	967	
remote-gateway statement.....	563	
usage guidelines.....	509	
remote-id statement.....	564	
usage guidelines.....	497	
remote-port-range statement		
PTSP.....	967	
remote-ports statement		
PTSP.....	968	
remote-prefix-list statement		
PTSP.....	968	
report-service-change statement.....	923	
request-timestamp statement.....	924	
request-url statement.....	1042	
required-depth statement.....	1275	
usage guidelines.....	1205	
retransmit-interval statement.....	603	
usage guidelines.....	584	
retry statement.....	1323	
usage guidelines.....	1299	
retry-delay statement.....	1323	
usage guidelines.....	1299	
RFC 2544 benchmarking test, RPM service		
configuring.....	1489	
example, configuring for Layer 3 IPv4		
services.....	1492	
example, configuring for NNI of Ethernet		
pseudowires.....	1507	
example, configuring for UNI of Ethernet		
pseudowires.....	1500	
overview.....	1468	
test name, configuring.....	1489	
test profile, configuring.....	1489	
RFC 2890.....	1570	
route-record statement		
usage guidelines.....	1151	
routing-instance statement		
BGF.....	924	
RPM.....	1543	
tunnel.....	1601	
usage guidelines.....	1577	
routing-instances statement.....	1601	
RPM.....	1543	
usage guidelines.....	1475	
routing-options statement.....	1602	
rpc-program-number statement.....	188	
usage guidelines.....	163	
RPM.....	1467	
example configuration.....	1516	
RPM services		
benchmarking test		
configuring.....	1489	
example, configuring for Layer 3 IPv4		
services.....	1492	
example, configuring for NNI of Ethernet		
pseudowires.....	1507	
example, configuring for UNI of Ethernet		
pseudowires.....	1500	
overview.....	1468	
rpm statement.....	1545	
RPM statements		
traceoptions.....	1555	
rtp statement.....	713, 925	
usage guidelines.....	697	
rule statement		
AACL.....	1072	
usage guidelines.....	1058	
APPID		
usage guidelines.....	997	
application identification.....	1046	
BGF.....	926	
CoS.....	733	
usage guidelines.....	717	
IDS.....	468	
usage guidelines.....	447	
IPsec.....	565	
usage guidelines.....	504	
NAT.....	327	
PTSP.....	969, 970	
software.....	345, 369	
stateful firewall.....	403	
usage guidelines.....	388	
rule-set statement		
AACL.....	1073	
usage guidelines.....	1062	
APPID		
usage guidelines.....	997	
application identification.....	1047	
BGF.....	926	
CoS.....	734	
usage guidelines.....	722	
IDS.....	469	
usage guidelines.....	453	
IPsec.....	566	
usage guidelines.....	511	
NAT.....	328, 1045	

PTSP.....	970
software.....	369
stateful firewall.....	404
usage guidelines.....	392
run-length statement.....	1276
usage guidelines.....	1136, 1186

## S

sample (firewall filter action).....	1135
sample-once statement	
flow monitoring.....	1276
usage guidelines.....	1137
sampled file.....	1140
sampled.pkts file.....	1138
sampling	
logical interface.....	1136
monitoring interface.....	1144
sampling rate.....	1136
sampling statement.....	1280
usage guidelines.....	1135
sbc-utils statement.....	927
scheduler map	
CoS	
configuration example.....	1395
secondary statement	
link services.....	692
usage guidelines.....	621
services PIC.....	826
usage guidelines.....	806
secure-nat-mapping statement.....	328
secured-port-block-allocation statement.....	329
security associations	
clearing.....	489
segmentation statement.....	928
senable-asymmetric-traffic-processing statement	
usage guidelines.....	1007
send cflowd records to flow collector.....	1300
send-notification-on-delay statement.....	929
server (PCP) statement.....	330
server statement.....	1546
server-inactivity-timeout statement.....	1546
service filters.....	804
service interface configuration.....	742
service packages.....	41
service rules configuration.....	747
service sets	
example configuration.....	759
overview.....	40

service statement.....	827
usage guidelines.....	803
service-change statement.....	930
service-change-type statement.....	931
service-domain statement.....	828
usage guidelines.....	744
service-filter statement.....	828
firewall	
usage guidelines.....	804
interfaces	
usage guidelines.....	742
service-interface statement.....	604, 782
BGF.....	931
usage guidelines.....	583, 742
service-interface-pools statement.....	952
service-port statement.....	1363
usage guidelines.....	1331
service-set statement.....	332, 783, 829, 1048
NAT.....	209
usage guidelines.....	741, 803
service-state statement	
virtual BGF.....	932
virtual interface in BGF.....	933
services configuration overview.....	46
services PICs.....	3
services statement	
AACL	
usage guidelines.....	1057
APPID	
usage guidelines.....	993
BGF.....	933
CoS.....	734
usage guidelines.....	715
DFC.....	1364
usage guidelines.....	1329
flow monitoring	
usage guidelines.....	1133
flow-monitoring.....	1281
IDS.....	469
usage guidelines.....	445
interfaces.....	830
usage guidelines.....	801
IPsec.....	566
usage guidelines.....	479
L2TP.....	605
usage guidelines.....	585
NAT.....	331
PTSP.....	971

- 
- rpm
    - usage guidelines.....1471
  - RPM.....1547
  - service sets.....786
    - usage guidelines.....754
  - stateful firewall.....404
    - usage guidelines.....387
  - services-options statement.....831
    - usage guidelines.....799, 801
  - session logging.....378
  - session-limit statement.....470, 832
    - usage guidelines.....450
  - session-mirroring statement.....934
  - session-timeout statement.....1051
    - usage guidelines.....995
  - set-dont-fragment-bit statement
    - IPsec.....567
    - service-set.....788
    - usage guidelines.....509
  - shaping-rate statement
    - usage guidelines.....632, 638, 643
  - shared-key statement.....1364
    - usage guidelines.....1331
  - short-sequence statement.....1460
    - usage guidelines.....1392
  - signature statement
    - nested applications.....1052
  - signature-method-all-ports statement.....1052
    - AAPID
      - usage guidelines.....1004
  - sip statement.....735
    - usage guidelines.....720
  - sip-call-hold-timeout statement.....188
  - size statement.....1281
    - usage guidelines.....1140
  - snmp-command statement.....189
    - usage guidelines.....162
  - soft-limit statement.....1365
    - usage guidelines.....1330
  - soft-limit-clear statement.....1365
    - usage guidelines.....1330
  - software-concentrator statement.....370
  - software-rules statement.....370
    - usage guidelines.....747
  - SONET interfaces
    - sampling SONET interfaces.....1141
  - source statement
    - AAPID
      - usage guidelines.....997
    - application identification rule.....1053
    - encryption.....1117
    - tunnel.....1602
    - usage guidelines.....1110, 1567
  - source-address statement
    - AACL.....1074
      - usage guidelines.....1059
    - BGF.....934
    - CoS.....735
      - usage guidelines.....718
    - flow monitoring.....1282
      - usage guidelines.....1145
    - IDS.....471
      - usage guidelines.....449
    - IPsec.....567
      - usage guidelines.....506
    - NAT.....334
      - usage guidelines.....205
    - RPM.....1547
    - service-set system log.....832
    - stateful firewall.....405
      - usage guidelines.....389
    - tunnel.....1603
    - tunnel services
      - usage guidelines.....1581
  - source-address-range statement
    - AACL.....1074
      - usage guidelines.....1059
    - IDS.....471
      - usage guidelines.....449
    - NAT.....334
      - usage guidelines.....205
    - stateful firewall.....405
      - usage guidelines.....389
  - source-addresses statement
    - DFC.....1366
      - usage guidelines.....1331
  - source-id statement.....1282
  - source-ipv4-address (RFC 2544
    - Benchmarking).....1548
  - source-pool statement.....335
    - usage guidelines.....206
  - source-port statement
    - BGF.....935
    - RPM.....189
      - usage guidelines.....152

source-prefix statement.....	335, 472	L2TP	
usage guidelines.....	450	usage guidelines.....	591
source-prefix-ipv6 statement.....	472	services	
usage guidelines.....	450	usage guidelines.....	1300
source-prefix-list statement		static destination address translation	
AACL.....	1075	configuring.....	221, 251
usage guidelines.....	1059	statistics statement	
CoS.....	736	L-PDF.....	1094
IDS.....	473	stop-detection-on-drop statement.....	936
NAT.....	336	support, technical See technical support	
stateful firewall.....	406	support-uni-directional-traffic statement.....	1053
usage guidelines.....	389	usage guidelines.....	1007
source-udp-port (RFC 2544 Benchmarking).....	1548	sustained-data-rate statement.....	937
spi statement.....	568	gate in packet gateway.....	938
usage guidelines.....	486	syn-cookie statement.....	473
stamp option.....	1140	usage guidelines.....	450
stamp statement.....	1283	syntax conventions.....	liii
usage guidelines.....	1138	syslog statement.....	422
state-loss statement.....	936	CoS.....	736
stateful firewall		usage guidelines.....	719
action statements.....	390	flow monitoring.....	1283
anomalies.....	50	IDS.....	474
applications.....	389	usage guidelines.....	450
example configuration.....	392	interfaces.....	833
match conditions.....	389	usage guidelines.....	801
overview.....	48	IPsec.....	568
restrictions.....	411	usage guidelines.....	508, 511
rules.....	392	L2TP.....	607
stateful firewall plug-in		usage guidelines.....	585
configuring memory for.....	411	NAT.....	336
stateful firewall use with APPID.....	999	service sets.....	789
stateful firewalls		usage guidelines.....	754
jservices-sfw package.....	409	stateful firewall.....	406
SDK Kerberos-enabled, configuring.....	411	usage guidelines.....	390
SDK plug-in for, loading.....	409	system log statement	
stateful NAT64		NAT	
configuring.....	238	usage guidelines.....	206
stateful-firewall-rule-sets statement			
usage guidelines.....	747	<b>T</b>	
stateful-firewall-rules statement.....	788	t391 statement.....	1460
usage guidelines.....	747	usage guidelines.....	1400
statement		t392 statement.....	1461
flow monitoring		usage guidelines.....	1400
usage guidelines.....	1140	target statement.....	1549
IPsec		RPM.....	1549
usage guidelines.....	517	tcp statement	
		RPM.....	1549
		tcp-mss statement.....	790
		tcp-tickles statement.....	833, 834

- technical support
  - contacting JTAC.....lv
- template statement
  - flow monitoring.....1284
- template-id statement.....1286
- template-refresh-rate statement.....1287
- term statement
  - ACL.....1076
    - usage guidelines.....1058
  - CoS.....737
    - usage guidelines.....717
  - HCM.....1043
  - IDS.....475
    - usage guidelines.....447
  - IPsec.....569
    - usage guidelines.....504
  - NAT.....338
  - PTSP
    - forward rule.....972
    - rule.....973
  - stateful firewall.....407
    - usage guidelines.....388
- test statement
  - RPM.....1550
- test-interface (RFC 2544 Benchmarking)
  - RPM.....1552
- test-interval statement.....1554
- test-name (RFC 2544 Benchmarking).....1553
- tests (RFC 2544 Benchmarking).....1551
- then statement
  - ACL.....1077
    - usage guidelines.....1058
  - CoS.....738
    - usage guidelines.....717
  - HCM.....1043
  - IDS.....477
    - usage guidelines.....447
  - IPsec.....570
    - usage guidelines.....504
  - NAT.....339
  - PTSP
    - forward rule.....974
    - rule.....975
  - stateful firewall.....408
    - usage guidelines.....388, 390
- threshold statement.....478
  - usage guidelines.....450
- thresholds statement
  - RPM.....1556
- time-to-live threshold.....163
- timerx statement.....939
- timestamp option.....1140
- tmax-retransmission-delay statement.....939
- topology
  - sample LFI and multilink bundle network.....1421
  - sample multilink bundle and LFI network.....1421
- trace-options
  - server (tracing flag).....758
  - timer-events (tracing flag).....758
- traceoptions statement
  - application identification.....1054
  - BGF.....940
  - flow monitoring.....1287
  - IPsec.....571
  - L-PDF.....1095
  - L2TP.....608
  - RPM.....1555
  - security.....573
  - services.....791
- tracing flags
  - event policy
    - all.....758, 1009
    - configuration.....758
    - database.....758
    - events.....758
    - policy.....758
    - server.....758
    - timer-events.....758
- tracing operations
  - adaptive services.....756
  - APPID.....1008
  - RPM.....1487
- traffic.....1103
  - inbound (decryption).....1107
  - IPsec, configuring.....1103
  - outbound (encryption).....1105
- traffic sampling
  - configuring.....1135
  - disabling.....1137, 1223
  - example configurations.....1141
  - flow aggregation.....1151
    - default values, option template ID.....1167
    - default values, template ID.....1167
    - observation domain ID, version 9.....1172
    - option template ID, version 9 and
      - IPFIX.....1167
    - source ID, IPFIX.....1172
    - template ID, version 9 and IPFIX.....1167

FTP traffic.....	1143	tunnel statement.....	1604
logging information output file.....	1140	encryption.....	1118
output files.....	1138	usage guidelines.....	1101
SONET interfaces.....	1141	redundancy	
traffic from single IP addresses.....	1142	usage guidelines.....	1110
traffic-control-profiles statement		unicast	
usage guidelines.....	638, 643	usage guidelines.....	1567
traffic-management statement.....	941	tunnel-group statement.....	612
transfer statement.....	1324	usage guidelines.....	582
usage guidelines.....	1298	tunnel-mtu statement.....	574, 793
transfer-log-archive statement.....	1324	usage guidelines.....	511, 752
usage guidelines.....	1299	tunnel-timeout statement.....	613
translated statement.....	340	usage guidelines.....	584
usage guidelines.....	206	tunnels	
translated-port statement		definition.....	1563
NAT.....	337	GRE	
translation-type statement.....	341	fragmentation of.....	1570
basic-nat-pt option.....	240	key number.....	1570
basic-nat44 option.....	212	interface types.....	1563
basic-nat66 option.....	217	IPv6-over-IPv4.....	1580, 1586
dnat-44 option, configuring.....	221, 251	twamp statement.....	1558
dynamic-nat44, configuring.....	225	twamp-server statement.....	1559
napt-44 option, configuring.....	229	twice NAT.....	56
napt-66 option, configuring.....	233	twice-napt-44 option	
napt-pt option, example.....	267	example.....	255
stateful-nat64 option, configuring.....	238	type statement.....	1055
usage guidelines.....	206	APPID	
traps statement.....	1557	usage guidelines.....	995
trigger-link-failure statement.....	693	type-of-service statement.....	1055
usage guidelines.....	618	APPID	
trusted-ca statement.....	792	usage guidelines.....	995
usage guidelines.....	750		
ttl statement		<b>U</b>	
DFC.....	1368	udp statement	
usage guidelines.....	1330	RPM.....	1559
tunnel.....	1603	undirectional traffic support	
usage guidelines.....	1567	APPID.....	1007
ttl-threshold statement.....	190	unicast tunnels.....	1567
usage guidelines.....	163	unit statement	
tunnel interfaces		aggregated Multiservices.....	443
configuration statements.....	1567, 1575, 1578	encryption.....	1119
dynamic tunnels.....	1581	usage guidelines.....	1101
example configuration.....	1584	flow monitoring.....	1288
logical tunnels.....	1576	usage guidelines.....	1135
loopback tunnels.....	1578	interfaces.....	835
multicast tunnels.....	1575	usage guidelines.....	795
PIM tunnels.....	1580		
unicast tunnels.....	1567		

link services.....	714, 1462
usage guidelines.....	1375
tunnel.....	1605
usage guidelines.....	1567
Universal Unique Identifier.....	163
up statement	
BGF.....	942
url statement.....	1056
APPID	
usage guidelines.....	1005
url-rule statement.....	1045
url_identifier, statement.....	1044
use-lower-case statement.....	942
use-wildcard-response statement.....	943
username statement	
flow collection.....	1325
usage guidelines.....	1299
uuid statement.....	190
usage guidelines.....	163
<b>V</b>	
v6rd statement.....	371
usage guidelines.....	344
var/log/sampled file.....	1140
var/tmp/sampled.pkts file.....	1138
variant statement.....	1325
usage guidelines.....	1298
version statement	
flow monitoring.....	1289
IKE.....	575
usage guidelines.....	494, 1152
version-ipfix statement.....	1292
usage guidelines.....	1176, 1181
version9 statement.....	1290
video statement.....	738
usage guidelines.....	720
virtual loopback tunnel	
configuration guidelines.....	1577
VRF table lookup	
example configuration.....	1586
virtual-interface statement.....	944
virtual-interface-down statement.....	945
virtual-interface-indications statement.....	946
virtual-interface-up statement.....	946
voice services	
bundles.....	700
configuration.....	695
encapsulation.....	699

example configuration.....	701
interface type.....	696
voice services interfaces	
interleave fragments.....	698
voice statement.....	739
usage guidelines.....	720
<b>W</b>	
warm standby	
AS PIC.....	806
LSQ PIC.....	621
warm statement.....	947
warm-standby statement.....	693
warning (system logging severity level).....	586, 755, 801
wired-process-mem-size statement.....	423
world-readable statement	
flow monitoring.....	1293
usage guidelines.....	1138

<b>Y</b>	
yellow-differential-delay statement.....	1463
usage guidelines.....	1399



# Index of Statements and Commands

## A

aacl-fields statement.....	1088
aacl-statistics-profile statement.....	1089
accounting statement	
flow monitoring.....	1216
acknowledge-retries statement.....	1442
acknowledge-timer statement.....	1443
action-red-differential-delay statement.....	1443
adaptive-services-pics statement.....	762
address statement	
application rule.....	1015
DFC.....	1349
encryption.....	1111
flow monitoring.....	1217
interfaces.....	814
link services.....	1444
NAT.....	307
voice services.....	706
address-allocation statement.....	307
address-range statement	
NAT.....	308
administrative statement	
BGF.....	847
aggregate-export-interval statement.....	1217
aggregation statement.....	457
flow monitoring.....	1218
algorithm statement.....	849
allow-fragmentation statement.....	1591
allow-ip-options statement.....	398
allow-multicast statement.....	763
allow-overlapping-nat-pools statement.....	308
allowed-destinations statement.....	1350
analyzer-address statement.....	1309
analyzer-id statement.....	1310
anti-replay-window-size statement.....	537, 764
app-mapping-timeout statement.....	309

application statement.....	180, 1016, 1017
application-aware-access-list-fields	
statement.....	1090
application-data-inactivity-detection	
statement.....	849
application-group statement.....	1017
application-group-any statement.....	1068
PTSP.....	956
application-groups statement.....	1018, 1068
PTSP.....	956
application-profile statement.....	726
application-protocol statement.....	181
application-set statement.....	182
application-sets statement	
CoS.....	727
IDS.....	458
NAT.....	309
stateful firewall.....	399
application-system-cache-timeout	
statement.....	1018
applications statement	
AACL.....	1067
application identification.....	1019
application-level gateways.....	399
applications hierarchy.....	183
CoS.....	727
IDS.....	458
NAT.....	310
PTSP.....	957
stateful firewall.....	399
archive-sites statement.....	1310
audit-observed-events-returns statement.....	850
authentication statement.....	538
authentication-algorithm statement	
IKE.....	539
IPsec.....	540
authentication-method statement.....	540
authentication-mode statement	
RPM.....	1521
automatic statement.....	1019
autonomous-system-type statement.....	1219
auxiliary-spi statement.....	541

## B

backup-destination statement.....	1592
backup-interface statement.....	1112
backup-remote-gateway statement.....	541
base-root statement.....	851
bgf-core statement.....	852

bgp statement	
RPM.....	1522
bundle statement.....	706, 1444
by-destination statement.....	459
by-pair statement.....	460
by-source statement.....	461
bypass-traffic-on-pic-failure statement.....	765, 1020

## C

cancel-graceful statement.....	854
capture-group statement.....	1351
cflowd statement.....	1220
cgn-pic statement.....	310, 815
chain-order statement	
nested applications.....	1020
cisco-interoperability statement.....	681
cleanup-timeout statement.....	855
clear-dont-fragment-bit statement	
GRE tunnel.....	815
IPsec.....	542
service-set.....	766
clear-ike-sas-on-pic-restart statement.....	542
clear-ipsec-sas-on-pic-restart statement.....	543
client-list statement.....	1523
collector statement.....	1311
compression statement.....	707
compression-device statement.....	707
content-destination statement.....	1352
context statement	
nested applications.....	1021
context-indications statement.....	856
control-association-indications statement.....	857
control-cores statement.....	413
control-source statement.....	1353
controller-address statement.....	858
controller-failure statement.....	858
controller-port statement.....	859
copy-dont-fragment-bit statement	
IPsec.....	543
service-set.....	767
copy-tos-to-outer-ip-header statement.....	1592
core-dump statement.....	1222
count-type statement	
PTSP.....	957

## D

data statement.....	728
data-cores statement.....	414
data-fill statement.....	1523

data-flow-affinity statement.....	414
data-format statement.....	1311
data-inactivity-detection statement.....	859
data-size statement.....	1524
default statement.....	860
delivery-function statement.....	861
demux statement	
PTSP.....	958
description statement	
IKE.....	544
IPsec.....	544
destination statement.....	415, 1113, 1445
application identification rule.....	1021
tunnel.....	1593
destination-address statement	
AACL.....	1069
BGF.....	861
CoS.....	728
IDS.....	462
IPsec.....	544
NAT.....	311
stateful firewall.....	400
destination-address-range statement	
AACL.....	1069
IDS.....	462
NAT.....	312
stateful firewall.....	400
destination-ipv4-address (RFC 2544	
Benchmarking).....	1525
destination-networks statement	
tunnel.....	1594
destination-pool statement.....	312
destination-port range statement	
NAT.....	313
destination-port statement	
applications.....	183
BGF.....	862
RPM.....	184, 1527
destination-prefix statement.....	313, 463
destination-prefix-ipv6 statement.....	463
destination-prefix-list statement	
AACL.....	1070
CoS.....	729
IDS.....	464
NAT.....	314
stateful firewall.....	401
destination-udp-port (RFC 2544	
Benchmarking).....	1528

destinations statement		
flow collection.....	1312	
destined-port statement		
NAT.....	314	
detect statement.....	862	
deterministic-port-block-allocation		
statement.....	315	
dh-group statement.....	545	
dial-options statement.....	817	
diffserv statement.....	863	
direction (RFC 2544 Benchmarking).....	1528	
direction statement.....	546	
nested applications.....	1022	
disable statement		
application.....	1023	
application group.....	1023	
flow monitoring.....	1223	
port mapping.....	1024	
disable-all-instances statement		
flow monitoring.....	1224	
disable-global-timeout-override statement.....	1024	
disable-mlppp-inner-ppp-pfc statement.....	1446	
disable-session-mirroring statement.....	863	
disconnect statement.....	864	
dlci statement.....	1446	
do-not-fragment statement		
tunnel.....	1595	
down statement.....	865	
download statement		
APPID.....	1025	
drop-member-traffic statement		
aggregated Multiservices.....	432	
drop-timeout statement.....	1447	
ds-lite statement.....	368	
dscp statement.....	729	
BGF.....	866	
dscp-code-point statement		
RPM.....	1529	
duplicates-dropped-periodicity statement.....	1354	
dynamic route insertion.....	513	
dynamic statement.....	547	
dynamic-flow-capture statement.....	1355	
dynamic-tunnels statement.....	1596	
<b>E</b>		
ei-mapping-timeout statement.....	317	
enable-asymmetric-traffic-processing		
statement.....	1026	
enable-heuristics statement.....	1025, 1026	
enable-rejoin statement		
aggregated Multiservices.....	433	
encapsulation statement.....	708	
link services.....	1448	
encoding statement.....	866	
encryption statement.....	548	
encryption-algorithm statement		
IKE.....	549	
IPsec.....	549	
engine-id statement		
flow monitoring.....	1224	
engine-type statement.....	1225	
es-options statement.....	1114	
event-timestamp-notification statement.....	867	
export-format statement.....	1227	
extension-provider statement.....	416	
extension-service statement.....	1226	
<b>F</b>		
f-max-period statement.....	708	
facility-override statement.....	597, 768, 818	
failover statement.....	869	
failover-cold statement.....	867	
failover-warm statement.....	868	
family (RFC 2544 Benchmarking).....	1530	
family statement		
aggregated Multiservices.....	433	
encryption.....	1115	
flow monitoring.....	1228	
interfaces.....	819	
link services.....	1450	
voice services.....	709	
fast-update-filters statement.....	870	
file statement.....	1234	
BGF.....	871	
L-PDF statistics.....	1091	
traffic sampling.....	1233	
file-specification statement.....	1313	
filename statement.....	1234	
filename-prefix statement.....	1312	
files statement.....	1235	
filter statement		
encryption.....	1116	
flow monitoring.....	1236	
flag statement.....	872	
flow-active-timeout statement.....	1237	
flow-collector statement.....	1314	
flow-control-options statement.....	1238	
flow-export-destination statement.....	1239	

flow-export-rate statement	
flow monitoring.....	1238
flow-inactive-timeout statement.....	1240
flow-monitoring statement.....	1241
flow-server statement	
flow monitoring.....	1242
flow-tap statement.....	1356
force-entry statement.....	464
forward-rule statement	
PTSP.....	960
forwarding instance.....	959
forwarding-class statement.....	682, 730
forwarding-db-size statement.....	417
forwarding-options statement.....	1243
fragment-threshold statement	
link services.....	1451
LSQ.....	683
voice services.....	710
fragmentation-map statement.....	683
fragmentation-maps statement.....	684
from statement	
ACL.....	1070
CoS.....	730
HCM.....	1041
IDS.....	465
IPsec.....	550
NAT.....	318
PTSP.....	961
PTSP forward rule.....	960
stateful firewall.....	402
ftp statement.....	731
flow collection.....	1316

## G

g-duplicates-dropped-periodicity statement.....	1357
g-max-duplicates statement.....	1358
gateway statement	
BGF.....	873
gateway-address statement.....	877
gateway-controller statement.....	878
gateway-port statement.....	879
graceful statement.....	880
graceful-restart statement.....	881

## H

h248-options statement.....	882
h248-profile statement.....	884
h248-properties statement.....	885
h248-stack statement.....	888

h248-timers statement.....	889
hanging-termination-detection statement.....	889
hard-limit statement.....	1358
hard-limit-target statement.....	1359
hardware-timestamp statement.....	1531
hash-key statement.....	418
hcm statement.....	1041
hello-interval statement	
L2TP.....	598
hello-timer statement	
link services.....	1451
hide-avps statement.....	599
high-availability-options statement	
aggregated Multiservices.....	434
history-size statement.....	1531
hold-time statement	
GRE tunnel interface.....	1597
host statement.....	769, 820
HCM.....	1042
L2TP.....	599
hot-standby statement.....	685, 820

## I

icmp-code statement.....	185
icmp-type statement.....	185
idle-timeout statement.....	1027
ids-rules statement.....	770
ignore-entry statement.....	464
ignore-errors statement.....	1027
ike statement.....	551
ike-access-profile statement.....	770
inactivity-delay statement.....	890
inactivity-duration statement.....	890
inactivity-non-tcp-timeout statement.....	1028
inactivity-tcp-timeout statement.....	1028
inactivity-timeout statement.....	186
BGF.....	891
flow monitoring.....	821
RPM.....	1532
inactivity-timer statement.....	892
index statement.....	1029
nested applications.....	1029
initial-average-ack-delay statement.....	892
initiate-dead-peer-detection statement.....	552
inline-jflow statement	
flow monitoring.....	1243
input statement	
flow monitoring.....	1244
interfaces.....	821

input-interface-index statement.....	1245
input-packet-rate-threshold statement.....	1359
instance statement	
port mirroring.....	1246
sampling.....	1247
interface statement	
flow monitoring.....	1249
flow-tap.....	1360
service interface pool.....	951
interface-map statement.....	1318
interface-service statement.....	771
interfaces statement	
aggregated Multiservices.....	435
DFC.....	1360
encryption.....	1116
flow monitoring.....	1251
interfaces hierarchy.....	822
link services.....	1452
tunnel.....	1597
voice services.....	710
interim-ah-scheme statement.....	893
interleave-fragments statement.....	1452
ip statement	
application identification.....	1030
ip-flow-stop-detection statement.....	893
ip-reassembly statement	
L2TP LNS.....	600
ip-reassembly-rules statement	
service-set.....	771
ipsec statement.....	553
ipsec-inside-interface statement.....	553
ipsec-sa statement	
encryption.....	1117
ipsec-transport-security-association	
statement.....	894
ipsec-vpn-options statement.....	772
ipsec-vpn-rules statement.....	772
ipv4-template statement.....	1251
ipv6-multicast-interfaces statement.....	319
ipv6-template statement.....	1252

## K

keepalive-time statement	
GRE tunnel interface.....	1598
key statement	
tunnel.....	1599

## L

L2TP statements	
LAC	
traceoptions.....	608
LNS	
ip-reassembly (service sets).....	600
ip-reassembly-rules.....	771
l2tp-access-profile.....	600
service-interface.....	604
traceoptions.....	608
l2tp-access-profile statement.....	600
label-position statement.....	1252
latch-deadlock-delay statement.....	894
learn-sip-register statement.....	186
lifetime-seconds statement	
IKE.....	554
IPsec.....	554
link-layer-overhead statement.....	685
lmi-type statement.....	1453
load-balancing-options statement	
aggregated Multiservices.....	436
local-address statement	
PTSP.....	962
local-address-range statement	
PTSP.....	963
local-certificate statement.....	554
local-dump statement.....	1253
local-gateway statement.....	601, 773
local-id statement.....	555
local-policy-decision-function statement.....	1092
local-port-range statement	
PTSP.....	963
local-ports statement	
PTSP.....	964
local-prefix-list statement	
PTSP.....	964
log-prefix statement.....	773, 822
L2TP.....	601
logging statement.....	466, 774
logical-system statement	
RPM.....	1532
lsq-failure-options statement.....	686

## M

manual statement.....	556
many-to-one statement	
aggregated Multiservices.....	437
mapping-timeout statement.....	320
match statement.....	1253

match-direction statement		mgc-segmentation-timer statement.....	910
AACL.....	1071	min-checked-bytes statement.....	1032
CoS.....	731	minimum-links statement.....	1453
IDS.....	466	minimum-priority statement.....	1361
IPsec.....	556	mlfr-uni-nni-bundle-options statement.....	1454
NAT.....	320	mode (RFC 2544 Benchmarking).....	1535
PTSP.....	965	mode statement.....	557
stateful firewall.....	402	monitor statement.....	911
max-burst-size statement.....	896	monitoring statement.....	1256
max-checked-bytes statement.....	1030	moving-average-size statement.....	1536
max-concurrent-calls statement.....	897	mpls-ipv4-template statement.....	1257
max-connection-duration statement.....	1533	mpls-template statement.....	1257
max-duplicates statement.....	1361	mrru statement.....	1455
max-flows statement.....	775	mss statement.....	467
max-packets-per-second statement.....	1255	mtu statement.....	1456
maximum-age statement.....	1319	multicast-dlci statement.....	1456
maximum-connections statement.....	1533	multicast-only statement.....	1599
maximum-connections-per-client		multilink-class statement.....	686
statement.....	1534	multilink-max-classes statement.....	687
maximum-contexts statement.....	711	multiservice-options statement.....	1258
maximum-fuf-percentage statement.....	898		
maximum-inactivity-time statement.....	899	<b>N</b>	
maximum-net-propagation-delay statement.....	900	n391 statement.....	1457
maximum-send-window statement.....	602	n392 statement.....	1458
maximum-sessions statement.....	1534	n393 statement.....	1459
maximum-sessions-per-connection		name-format statement.....	1320
statement.....	1535	nat-options statement.....	777
maximum-synchronization-mismatches		nat-rules statement.....	777
statement.....	900	nested-application statement	
maximum-terms statement.....	901	APPID.....	1033
maximum-transactions statement		nested-application-settings statement	
nested applications.....	1031	APPID.....	1034
maximum-waiting-delay statement.....	901	network-operator-id statement.....	911
media statement.....	902	next-hop statement.....	1258
member statement		next-hop-group statement	
nested applications.....	1031	forwarding-options.....	1259
member-failure-options statement		port mirroring.....	1260
aggregated Multiservices.....	438	next-hop-service statement.....	778
member-interface statement		no-anti-replay statement.....	557, 779
aggregated Multiservices.....	440	no-application-identification statement.....	1034
mg-maximum-pdu-size statement.....	903	no-application-system-cache statement.....	1035
mg-originated-pending-limit statement.....	904	no-clear-application-system-cache	
mg-provisional-response-timer-value		statement.....	1035
statement.....	905	no-core-dump statement.....	1222
mg-segmentation-timer statement.....	906	no-dscp-bit-mirroring statement.....	912
mgc-maximum-pdu-size statement.....	907	no-filter-check statement.....	1260
mgc-originated-pending-limit statement.....	908	no-fragmentation statement.....	688
mgc-provisional-response-timer-value		no-ipsec-tunnel-in-traceroute statement.....	558
statement.....	909	no-local-dump statement.....	1253

no-nested-application statement.....	1036
no-per-unit-scheduler statement.....	688
no-protocol-method statement.....	1036
no-remote-trace statement	
flow monitoring.....	1261
no-rtcp-check statement.....	912
no-signature-based statement.....	1037
no-stamp statement.....	1283
no-syslog statement	
DFC.....	1362
flow monitoring.....	1283
no-termination-request statement.....	689
no-translation statement.....	321
no-world-readable statement	
flow monitoring.....	1293
normal-mg-execution-time statement.....	913
normal-mgc-execution-time statement.....	914
notification-behavior statement.....	915
notification-rate-limit statement.....	915
notification-regulation statement.....	916
notification-targets statement.....	1362
<b>O</b>	
object-cache-size statement.....	419
observation-domain-id statement.....	1262
one-way-hardware-timestamp statement.....	1536
open-timeout statement.....	823
option-refresh-rate statement.....	1263
options-template-id statement.....	1264
order statement.....	1037
output statement.....	824
discard accounting.....	1265
flow monitoring.....	1266
port mirroring.....	1267
sampling.....	1268
output-interface-index statement.....	1269
overload-control statement.....	916
overload-pool statement.....	321
overload-prefix statement.....	322
<b>P</b>	
package statement	
loading on PIC.....	420
passive-mode-tunneling statement.....	780
passive-monitor-mode statement.....	1270
password statement	
flow collection.....	1322
pattern statement	
nested applications.....	1038
peak-data-rate statement.....	917, 918
peer-unit statement	
tunnel.....	1600
per-unit-scheduler statement.....	690
perfect-forward-secrecy statement.....	558
pgcp-rules statement	
service-set.....	780
pic-memory-threshold statement.....	1363
platform statement.....	919
policy statement	
IKE.....	559
policy-db-size statement.....	421
policy-decision-statistics-profile statement.....	1093
pool statement.....	323
service interface pool.....	952
pop-all-labels statement.....	1271
port statement	
flow monitoring.....	1272
NAT.....	324
RPM.....	1537
TWAMP.....	1537
voice services.....	712
port-forwarding statement	
destined-port statement.....	314
NAT.....	325
translated-port statement.....	337
port-mapping statement.....	1038
port-mirroring statement.....	1273
port-range statement.....	1039
ports-per-session statement.....	326
post-service-filter statement.....	824
ppp-access-profile statement.....	602
pre-shared-key statement.....	560
preserve-interface statement.....	691
primary statement	
link services.....	691
services PIC.....	825
probe statement	
RPM.....	1538
probe-count statement.....	1539
probe-interval statement.....	1539
probe-limit statement.....	1540
probe-server statement.....	1541
probe-type statement.....	1542
profile statement	
application identification.....	1039
profile-name statement.....	920
profile-version statement.....	920

proposal statement	1600
IKE.....	561
IPsec.....	562
proposals statement	
IKE.....	562
IPsec.....	562
protocol statement	
applications.....	187
IPsec.....	563
nested applications.....	1040
PTSP.....	965
PTSP statements	
application-group-any.....	956
application-groups.....	956
applications.....	957
count-type.....	957
demux.....	958
forward-rule	
.....	960
forwarding instance.....	959
local-address.....	962
local-address-range.....	963
local-port-range.....	963
local-ports.....	964
local-prefix-list.....	964
match-direction.....	965
protocol.....	965
remote-address.....	966
remote-address-range.....	967
remote-port-range.....	967
remote-ports.....	968
remote-prefix-list.....	968
rule-set.....	970
services.....	971
term	
forward rule.....	972
rule.....	973
then	
forward rule.....	974
rule.....	975
ptsp-rules statement.....	781
<b>Q</b>	
queue-limit-percentage statement.....	921
queues statement.....	712
<b>R</b>	
random-allocation statement.....	324
rate statement.....	825, 1274
reassemble-packets statement.....	1274
receive-options-packets statement.....	1275
receive-ttl-exceeded statement.....	603
receive-window statement.....	922
reconnect statement.....	1459
red-differential-delay statement.....	
redistribute-all-traffic statement	
aggregated Multiservices.....	441
redundancy-options statement.....	692, 826
reflexive   reverse statement.....	732
reject-all-commands-threshold statement.....	922
reject-new-calls-threshold statement.....	923
rejoin-timeout statement	
aggregated Multiservices.....	442
remote-address statement	
PTSP.....	966
remote-address-range statement	
PTSP.....	967
remote-gateway statement.....	563
remote-id statement.....	564
remote-port-range statement	
PTSP.....	967
remote-ports statement	
PTSP.....	968
remote-prefix-list statement	
PTSP.....	968
report-service-change statement.....	923
request-timestamp statement.....	924
request-url statement.....	1042
required-depth statement.....	1275
retransmit-interval statement.....	603
retry statement.....	1323
retry-delay statement.....	1323
routing-instance statement	
BGF.....	924
RPM.....	1543
tunnel.....	1601
routing-instances statement.....	1601
RPM.....	1543
routing-options statement.....	1602
rpc-program-number statement.....	188
rpm statement.....	1545
RPM statements	
traceoptions.....	1555
rtp statement.....	713, 925
rule statement	
AACL.....	1072
application identification.....	1046
BGF.....	926

CoS.....	733	services statement	
IDS.....	468	BGF.....	933
IPsec.....	565	CoS.....	734
NAT.....	327	DFC.....	1364
PTSP.....	969, 970	flow-monitoring.....	1281
software.....	345, 369	IDS.....	469
stateful firewall.....	403	interfaces.....	830
rule-set statement		IPsec.....	566
AACL.....	1073	L2TP.....	605
application identification.....	1047	NAT.....	331
BGF.....	926	PTSP.....	971
CoS.....	734	RPM.....	1547
IDS.....	469	service sets.....	786
IPsec.....	566	stateful firewall.....	404
NAT.....	328, 1045	services-options statement.....	831
PTSP.....	970	session-limit statement.....	470, 832
software.....	369	session-mirroring statement.....	934
stateful firewall.....	404	session-timeout statement.....	1051
run-length statement.....	1276	set-dont-fragment-bit statement	
		IPsec.....	567
<b>S</b>		service-set.....	788
sample-once statement		shared-key statement.....	1364
flow monitoring.....	1276	short-sequence statement.....	1460
sampling statement.....	1280	signature statement	
sbc-utils statement.....	927	nested applications.....	1052
secondary statement		sip statement.....	735
link services.....	692	sip-call-hold-timeout statement.....	188
services PIC.....	826	size statement.....	1281
secured-port-block-allocation statement.....	329	snmp-command statement.....	189
segmentation statement.....	928	soft-limit statement.....	1365
send-notification-on-delay statement.....	929	soft-limit-clear statement.....	1365
server (PCP) statement.....	330	software-concentrator statement.....	370
server statement.....	1546	software-rules statement.....	370
server-inactivity-timeout statement.....	1546	source statement	
service statement.....	827	application identification rule.....	1053
service-change statement.....	930	encryption.....	1117
service-change-type statement.....	931	tunnel.....	1602
service-domain statement.....	828	source-address statement	
service-filter statement.....	828	AACL.....	1074
service-interface statement.....	604, 782	BGF.....	934
BGF.....	931	CoS.....	735
service-interface-pools statement.....	952	flow monitoring.....	1282
service-port statement.....	1363	IDS.....	471
service-set statement.....	332, 783, 829, 1048	IPsec.....	567
service-state statement		NAT.....	334
virtual BGF.....	932	RPM.....	1547
virtual interface in BGF.....	933	stateful firewall.....	405
		tunnel.....	1603

source-address-range statement	
AACL.....	1074
IDS.....	471
NAT.....	334
stateful firewall.....	405
source-addresses statement	
DFC.....	1366
source-id statement.....	1282
source-ipv4-address (RFC 2544	
Benchmarking).....	1548
source-pool statement.....	335
source-port statement	
BGF.....	935
RPM.....	189
source-prefix statement.....	335, 472
source-prefix-ipv6 statement.....	472
source-prefix-list statement	
AACL.....	1075
CoS.....	736
IDS.....	473
NAT.....	336
stateful firewall.....	406
source-udp-port (RFC 2544 Benchmarking).....	1548
spi statement.....	568
stamp statement.....	1283
state-loss statement.....	936
stateful-firewall-rules statement.....	788
statistics statement	
L-PDF.....	1094
stop-detection-on-drop statement.....	936
support-uni-directional-traffic statement.....	1053
sustained-data-rate statement.....	937
gate in packet gateway.....	938
syn-cookie statement.....	473
syslog statement.....	422
CoS.....	736
flow monitoring.....	1283
IDS.....	474
interfaces.....	833
IPsec.....	568
L2TP.....	607
NAT.....	336
service sets.....	789
stateful firewall.....	406

## T

t391 statement.....	1460
t392 statement.....	1461

target statement.....	1549
RPM.....	1549
tcp statement	
RPM.....	1549
tcp-mss statement.....	790
tcp-tickles statement.....	833, 834
template statement	
flow monitoring.....	1284
template-id statement.....	1286
template-refresh-rate statement.....	1287
term statement	
AACL.....	1076
CoS.....	737
HCM.....	1043
IDS.....	475
IPsec.....	569
NAT.....	338
PTSP	
forward rule.....	972
rule.....	973
stateful firewall.....	407
test statement	
RPM.....	1550
test-interface (RFC 2544 Benchmarking)	
RPM.....	1552
test-interval statement.....	1554
test-name (RFC 2544 Benchmarking).....	1553
tests (RFC 2544 Benchmarking).....	1551
then statement	
AACL.....	1077
CoS.....	738
HCM.....	1043
IDS.....	477
IPsec.....	570
NAT.....	339
PTSP	
forward rule.....	974
rule.....	975
stateful firewall.....	408
threshold statement.....	478
thresholds statement	
RPM.....	1556
timerx statement.....	939
tmax-retransmission-delay statement.....	939
traceoptions statement	
application identification.....	1054
BGF.....	940
flow monitoring.....	1287
IPsec.....	571

L-PDF.....	1095
L2TP.....	608
RPM.....	1555
security.....	573
services.....	791
traffic-management statement.....	941
transfer statement.....	1324
transfer-log-archive statement.....	1324
translated statement.....	340
translated-port statement	
NAT.....	337
traps statement.....	1557
trigger-link-failure statement.....	693
trusted-ca statement.....	792
ttl statement	
DFC.....	1368
tunnel.....	1603
ttl-threshold statement.....	190
tunnel statement.....	1604
encryption.....	1118
tunnel-group statement.....	612
tunnel-mtu statement.....	574, 793
tunnel-timeout statement.....	613
twamp statement.....	1558
twamp-server statement.....	1559
type statement.....	1055
type-of-service statement.....	1055

## U

udp statement	
RPM.....	1559
unit statement	
aggregated Multiservices.....	443
encryption.....	1119
flow monitoring.....	1288
interfaces.....	835
link services.....	714, 1462
tunnel.....	1605
up statement	
BGF.....	942
url statement.....	1056
url-rule statement.....	1045
url_identifier, statement.....	1044
use-lower-case statement.....	942
use-wildcard-response statement.....	943
username statement	
flow collection.....	1325
uuid statement.....	190

## V

v6rd statement.....	371
variant statement.....	1325
version statement	
flow monitoring.....	1289
IKE.....	575
version-ipfix statement.....	1292
version9 statement.....	1290
video statement.....	738
virtual-interface statement.....	944
virtual-interface-down statement.....	945
virtual-interface-indications statement.....	946
virtual-interface-up statement.....	946
voice statement.....	739

## W

warm statement.....	947
warm-standby statement.....	693
wired-process-mem-size statement.....	423
world-readable statement	
flow monitoring.....	1293

## Y

yellow-differential-delay statement.....	1463
--	------

