



Junos[®] OS

Monitoring, Sampling, and Collection Services Interfaces Feature Guide for Routing Devices

Release
15.1



Modified: 2016-11-09

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
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[®] OS Monitoring, Sampling, and Collection Services Interfaces Feature Guide for Routing Devices

15.1

Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

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.

Table of Contents

	About the Documentation	xxi
	Documentation and Release Notes	xxi
	Supported Platforms	xxi
	Using the Examples in This Manual	xxi
	Merging a Full Example	xxii
	Merging a Snippet	xxii
	Documentation Conventions	xxiii
	Documentation Feedback	xxv
	Requesting Technical Support	xxv
	Self-Help Online Tools and Resources	xxv
	Opening a Case with JTAC	xxvi
Part 1	Flow Monitoring and Flow Collection Services	
Chapter 1	Monitoring Traffic Using Active Flow Monitoring	3
	Active Flow Monitoring Overview	3
	Configuring Flow Monitoring	6
	Configuring Flow-Monitoring Interfaces	6
	Configuring Flow-Monitoring Properties	8
	Directing Traffic to Flow-Monitoring Interfaces	8
	Exporting Flows	9
	Configuring Time Periods when Flow Monitoring is Active and Inactive	9
	Example: Configuring Flow Monitoring	10
	Example: Configuring Active Monitoring on Logical Systems	11
	Example: Configuring Flow Monitoring on MS-MIC and MS-MPC	14
	Configuring Services Interface Redundancy with Flow Monitoring	21
	Flow Offloading	23
Chapter 2	Monitoring Traffic Using Passive Flow Monitoring	25
	Passive Flow Monitoring Overview	25
	Enabling Passive Flow Monitoring	26
	Passive Flow Monitoring for MPLS Encapsulated Packets	28
	Removing MPLS Labels from Incoming Packets	29
	Example: Enabling IPv4 Passive Flow Monitoring	30
	Example: Enabling IPv6 Passive Flow Monitoring	32
Chapter 3	Processing and Exporting Multiple Records Using Flow Collection	35
	Flow Collection Overview	35
	Configuring Flow Collection	36
	Configuring Destination FTP Servers for Flow Records	36
	Configuring a Packet Analyzer	37

	Configuring File Formats	37
	Configuring Interface Mappings	38
	Configuring Transfer Logs	38
	Configuring Retry Attempts	39
	Example: Configuring Flow Collection	40
	Sending cflowd Records to Flow Collector Interfaces	46
	Configuring Flow Collection Mode and Interfaces on Services PICs	46
Chapter 4	Logging Flow Monitoring Records With Version 9 and IPFIX Templates for NAT Events	47
	Logging NAT Events in Flow Monitoring Format Overview	48
	Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format	57
	Exporting Syslog Messages to an External Host Without Flow Monitoring Formats Overview	58
	Exporting Version 9 Flow Data Records to a Log Collector Overview	59
	Exporting IPFIX Flow Data Records to a Log Collector Overview	60
	Mapping Between Field Values for Version 9 Flow Templates and Logs Exported	61
	Mapping Between Field Values for IPFIX Flow Templates and Logs Exported	64
	Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats	68
	Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting	69
Part 2	Flow Capture Services	
Chapter 5	Dynamically Capturing Packet Flows Using Junos Capture Vision	79
	Understanding Junos Capture Vision	79
	Junos Capture Vision Architecture	79
	Liberal Sequence Windowing	80
	Intercepting IPv6 Flows	81
	Configuring Junos Capture Vision	81
	Configuring the Capture Group	81
	Configuring the Content Destination	82
	Configuring the Control Source	83
	Configuring the DFC PIC Interface	84
	Configuring the Firewall Filter	85
	Configuring System Logging	85
	Configuring Tracing Options for Junos Capture Vision Events	86
	Configuring Thresholds	86
	Limiting the Number of Duplicates of a Packet	87
	Example: Configuring Junos Capture Vision	87
Chapter 6	Detecting Threats and Intercepting Flows Using Junos Packet Vision	91
	Understanding Junos Packet Vision	91
	Junos Packet Vision Architecture	92
	Configuring Junos Packet Vision	93
	Configuring the Junos Packet Vision Interface	93
	Strengthening Junos Packet Vision Security	94

	Restrictions on Junos Packet Vision Services	95
	Configuring FlowTapLite	96
	Examples: Configuring Flow-Tap Services	97
Part 3	Sampling, Discard Accounting, and Port Mirroring Services	
Chapter 7	Sampling Data Using Traffic Sampling and Discard Accounting	103
	Configuring Traffic Sampling	103
	Configuring Firewall Filter for Traffic Sampling	104
	Configuring Traffic Sampling on a Logical Interface	105
	Disabling Traffic Sampling	107
	Sampling Once	107
	Preserving Prerewrite ToS Value for Egress Sampled or Mirrored Packets	107
	Configuring Traffic Sampling Output	108
	Traffic Sampling Output Format	110
	Tracing Traffic Sampling Operations	110
	Traffic Sampling Examples	111
	Example: Sampling a Single SONET/SDH Interface	111
	Example: Sampling All Traffic from a Single IP Address	112
	Example: Sampling All FTP Traffic	113
	Sampling Instance Configuration	114
	Configuring Discard Accounting	115
Chapter 8	Sampling Data Using Inline Sampling	117
	Understanding Inline Active Flow Monitoring	117
	Inline Active Flow Monitoring	117
	Inline Active Flow Monitoring Limitations and Restrictions	118
	IPFIX and Version 9 Templates	120
	Fields Included in the IPFIX IPv4 Template	120
	Fields Included in the IPFIX IPv6 Template	121
	Fields Included in the Version 9 IPv4 Template	121
	Configuring Inline Active Flow Monitoring	122
	Configuring Inline Active Flow Monitoring on MX80 Routers	125
	Monitoring Network Traffic Flow Using Inline Flow Monitoring on PTX Series Routers	127
Chapter 9	Sampling Data Using Flow Aggregation	131
	Understanding Flow Aggregation	131
	Enabling Flow Aggregation	132
	Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd	132
	Configuring Flow Aggregation to Use Version 9 Flow Templates	137
	Configuring the Traffic to Be Sampled	137
	Configuring the Version 9 Template Properties	138
	Customizing Template ID, Observation Domain ID, and Source ID for Version 9 flow Templates	139
	Restrictions	140
	Fields Included in Each Template Type	141
	MPLS Sampling Behavior	142
	Verification	143

Examples: Configuring Version 9 Flow Templates	143
Configuring Flow Aggregation to Use IPFIX Flow Templates	147
Configuring the IPFIX Template Properties	147
Restrictions	148
Customizing Template ID, Observation Domain ID, and Source ID for IPFIX flow Templates	148
Fields Included in the IPv4 Template	149
Fields Included in the IPv6 Template	150
Verification	151
Example: Configuring an IPFIX Flow Templates and Flow Sampling	151
Configuring Flow Aggregation to Use IPFIX Flow Templates on PTX Series Routers	152
Configuring the IPFIX Template Properties	152
Restrictions	153
Customizing Template ID, Observation Domain ID, and Source ID for IPFIX flow Templates	153
Fields Included in the IPv4 Templates for PTX Series Routers	154
Fields Included in the IPv6 Templates for PTX Series Routers	155
Verification	156
Example: Configuring an IPFIX Flow Templates and Flow Sampling	156
Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows	157
Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows	160
Inclusion of Fragmentation Identifier and IPv6 Extension Header Elements in IPFIX Templates	165
Directing Replicated Flows to Multiple Flow Servers	167
Directing Replicated Routing Engine–Based Sampling Flows to Multiple Servers	168
Directing Replicated Version 9 Flow Aggregates to Multiple Servers	168
Logging cflowd Flows Before Export	170
Chapter 10	
Sending Packets for Analysis Using Port Mirroring	173
Understanding Port Mirroring	173
Configuring Port Mirroring	173
Configuring Tunnels	176
Port Mirroring with Next-Hop Groups	178
Configuring Inline Port Mirroring	179
Filter-Based Forwarding with Multiple Monitoring Interfaces	180
Restrictions	180
Configuring Port Mirroring on Services Interfaces	181
Examples: Configuring Port Mirroring	182
Defining a Next-Hop Group for Port Mirroring	190
Example: Multiple Port Mirroring with Next-Hop Groups Configuration	191

Part 4	Real-Time Performance Monitoring and Video Monitoring Services	
Chapter 11	Monitoring Traffic Using Real-Time Performance Monitoring	199
	Real-Time Performance Monitoring Services Overview	199
	Two-Way Active Measurement Protocol Overview	201
	TWAMP on MX series routers	201
	Configuring RPM Probes	201
	Configuring RPM Receiver Servers	206
	Limiting the Number of Concurrent RPM Probes	206
	Configuring RPM Timestamping	207
	Configuring TWAMP	210
	Configuring TWAMP Interfaces	210
	Configuring TWAMP Servers	210
	Configuring BGP Neighbor Discovery Through RPM	211
	Examples: Configuring BGP Neighbor Discovery Through RPM	214
	Tracing RPM Operations	215
	Configuring the RPM Log File Name	216
	Configuring the Number and Size of RPM Log Files	216
	Configuring Access to the Log File	216
	Configuring a Regular Expression for Lines to Be Logged	216
	Configuring the Trace Operations	217
	Examples: Configuring Real-Time Performance Monitoring	217
	Enabling RPM for the Services SDK	221
Chapter 12	Managing License Server for Throughput Data Export	223
	License Server Management for Throughput Data Export for NAT, Firewall, and Inline Flow Monitoring Services	223
	Throughput Measurement and Export	224
	Guidelines for Configuring Transmission of Per-Service Throughput to an External Log Collector	225
Chapter 13	Testing the Performance of Network Devices Using RFC 2544-Based Benchmarking	227
	RFC2544-Based Benchmarking Tests Overview	227
	RFC2544-Based Benchmarking Tests for E-LAN and E-Line Services Overview	231
	Supported RFC2544-Based Benchmarking Statements on MX104 Routers	234
	Configuring an RFC 2544-Based Benchmarking Test	235
	Configuring a Test Name for an RFC 2544-Based Benchmarking Test for a IPv4 Network	235
	Configuring a Test Name for an RFC 2544-Based Benchmarking Test for an Ethernet Pseudowire	237
	Configuring a Test Name for an RFC 2544-Based Benchmarking Test for a Layer 2 E-LAN Service in Bridge Domain	238
	Example: Configuring an RFC 2544-Based Benchmarking Test for Layer 3 IPv4 Services	239
	Example: Configuring an RFC 2544-Based Benchmarking Test for UNI Direction of Ethernet Pseudowires	246

	Example: Configuring an RFC 2544-Based Benchmarking Test for NNI Direction of Ethernet Pseudowires	254
	Example: Configuring RFC2544-Based Benchmarking Tests for Layer 2 E-LAN Services in Bridge Domains	262
	Example: Configuring Benchmarking Tests to Measure SLA Parameters for E-LAN Services Using VPLS	287
Chapter 14	Tracking Streaming Media Traffic Using Inline Video Monitoring	309
	Inline Video Monitoring Overview	309
	Configuring Inline Video Monitoring	311
	Configuring Media Delivery Indexing Criteria	312
	Configuring Interface Flow Criteria	313
	Inline Video Monitoring Syslog Messages	314
	Generation of SNMP Traps and Alarms for Inline Video Monitoring	314
	Collection of MDI Statistics Associated with an FPC Slot	315
	Collection of MDI Errors Associated with an FPC Slot	315
	Collection of MDI Flows Associated with an FPC Slot	316
	Collection of MDI Record-Level Metrics	317
	SNMP Traps for Inline Video Monitoring Statistics	317
	Processing SNMP GET Requests for MDI Metrics	318
Part 5	Configuration Statements and Operational Commands	
Chapter 15	Configuration Statements	321
	[edit forwarding-options] Hierarchy Level	328
	[edit interfaces] Hierarchy Level	331
	[edit services dynamic-flow-control] Hierarchy Level	332
	[edit services flow-collector] Hierarchy Level	333
	[edit services flow-monitoring] Hierarchy Level	334
	[edit services flow-tap] Hierarchy Level	335
	[edit services rpm] Hierarchy Level	335
	accounting	338
	address (Interfaces)	339
	address (Services Dynamic Flow Capture)	339
	aggregate-export-interval	340
	aggregation	341
	alarms	342
	alarm-mode	343
	allowed-destinations	344
	analyzer-address	344
	analyzer-id	345
	archive-sites	345
	authentication-mode	346
	authentication-key-chain (TWAMP)	347
	autonomous-system-type	348
	bgp	349
	capture-group	350
	cflowd (Discard Accounting)	351
	cflowd (Flow Monitoring)	352
	client	353

client-list	354
collector	354
collector (Flow Monitoring Logs for NAT)	355
collector (Flow Template Profiles for NAT)	356
collector-group (Flow Template Profiles for NAT)	357
collector-group (Flow Monitoring Logs for NAT)	358
content-destination	359
control-connection	360
control-source	361
core-dump	362
data-fill	363
data-fill-with zeros	364
data-format	364
data-size	365
delay-factor	366
destination (Interfaces)	367
destination-address (Flow Monitoring Logs for NAT)	368
destination-interface	369
destination-ipv4-address (RFC 2544 Benchmarking)	370
destination-mac-address (RFC2544 Benchmarking)	371
destination-port	372
destination-port (Flow Monitoring Logs for NAT)	373
destination-udp-port (RFC 2544 Benchmarking)	373
destinations	374
direction (RFC2544 Benchmarking)	375
disable (Forwarding Options)	376
disable-signature-check (RFC 2544 Benchmarking)	377
dscp-code-point	378
duplicates-dropped-periodicity	379
dynamic-flow-capture	380
engine-id (Forwarding Options)	381
engine-type	382
export-format	383
extension-service	384
family (Monitoring)	386
family (Port Mirroring)	387
family (RFC2544 Benchmarking)	388
family (Sampling)	389
file (Sampling)	390
file (Trace Options)	391
file-specification (File Format)	391
file-specification (Interface Mapping)	392
filename	392
filename-prefix	393
files	393
filter	394
flow-active-timeout	395
flow-collector	396
flow-export-destination	397

flow-export-rate	397
flow-inactive-timeout	398
flow-monitoring	399
flow-server	400
flow-table-size	401
flow-tap	402
ftp (Flow Collector Files)	403
ftp (Transfer Log Files)	404
g-duplicates-dropped-periodicity	404
g-max-duplicates	405
generate-snmp-traps	405
hard-limit	406
hard-limit-target	406
hardware-timestamp	407
history-size	407
host-outbound	408
in-service (RFC2544 Benchmarking)	409
inactivity-timeout (Services RPM)	409
inline-jflow	410
input (Port Mirroring)	410
input (Sampling)	411
input-interface-index	411
input-packet-rate-threshold	412
instance (Sampling)	413
interface (Accounting or Sampling)	414
interfaces	415
interface (Services Flow Tap)	415
interface-map	416
interfaces (Services Dynamic Flow Capture)	416
interfaces (Video Monitoring)	417
inet6-options (Services)	418
ip-swap (RFC 2544 Benchmarking)	418
ipv4-flow-table-size	419
ipv4-template	419
ipv6-flow-table-size	420
ipv6-extended-attrib	420
ipv6-template	421
jflow-log (Interfaces)	422
jflow-log (Services)	423
label-position	424
license-server	425
local-dump	426
logical-system	426
match	427
max-connection-duration	427
max-duplicates	428
max-packets-per-second	429
maximum-age	429
maximum-connections	430

maximum-connections-per-client	431
maximum-packet-length	432
maximum-sessions	433
maximum-sessions-per-connection	434
media-loss-rate	435
media-rate-variation	436
message-rate-limit (Flow Monitoring Logs for NAT)	437
minimum-priority	438
mode (RFC 2544 Benchmarking)	438
monitoring	439
moving-average-size	440
mpls-ipv4-template	440
mpls-template	441
multiservice-options	441
name-format	442
next-hop (Forwarding Options)	443
next-hop-group (Forwarding Options)	444
next-hop-group (Port Mirroring)	445
no-filter-check	445
no-remote-trace (Trace Options)	446
no-syslog	446
no-syslog-generation	447
notification-targets	447
observation-domain-id	448
one-way-hardware-timestamp	449
option-refresh-rate	450
options-template-id	451
output (Accounting)	452
output (Monitoring)	453
output (Port Mirroring)	454
output (Sampling)	455
output-interface-index	456
passive-monitor-mode	456
password (Flow Collector File Servers)	457
password (Transfer Log File Servers)	457
peer-as-billing-template	458
pic-memory-threshold	458
pop-all-labels	459
port (Flow Monitoring)	460
port (RPM)	460
port (TWAMP)	461
port-mirroring	462
post-cli-implicit-firewall	463
pre-rewrite-tos	464
probe	465
probe-count	466
probe-interval	467
probe-limit	467
probe-server	468

probe-type	469
rate (Forwarding Options)	470
receive-options-packets	471
receive-ttl-exceeded	471
refresh-rate (Flow Monitoring Logs for NAT)	472
reflect-mode (RFC2544 Benchmarking)	473
reflect-etype (RFC 2544 Benchmarking)	474
required-depth	475
retry (Services Flow Collector)	476
retry-delay	476
rfc2544-benchmarking	477
routing-instance	478
routing-instance (cflowd)	479
routing-instance-list (TWAMP)	480
routing-instances	481
rpm (Interfaces)	482
rpm (Services)	483
run-length	485
sample-once	485
sampling (Forwarding Options)	486
sampling (Interfaces)	488
server	489
server-inactivity-timeout	489
service-port	490
service-type (RFC2544 Benchmarking)	490
services	491
services	491
services-options	492
shared-key	493
size	493
soft-limit	494
soft-limit-clear	494
source-address (Forwarding Options)	495
source-address (Services)	496
source-addresses	496
source-id	497
source-ip (Flow Monitoring Logs for NAT)	498
source-ipv4-address (RFC 2544 Benchmarking)	499
source-mac-address (RFC2544 Benchmarking)	499
source-udp-port (RFC 2544 Benchmarking)	500
stamp	500
storm-control	501
syslog	501
target (Services RPM)	502
tcp	503
templates	504
test	506
tests (RFC 2544 Benchmarking)	507
test-interface (RFC 2544 Benchmarking)	508

test-interval	509
test-name (RFC 2544 Benchmarking)	510
test-session	511
thresholds	512
traceoptions (Dynamic Flow Capture)	513
traceoptions (Forwarding Options)	514
traceoptions (RPM)	515
transfer	516
transfer-log-archive	517
traps	518
ttl	519
twamp	520
twamp-server	521
template (Forwarding Options)	521
template-id	522
template-profile (Flow Monitoring Logs for NAT)	523
template-refresh-rate	524
template-type (Flow Monitoring Logs for NAT)	525
trio-flow-offload	526
udp	526
udp-tcp-port-swap (RFC 2544 Benchmarking)	527
unit	528
username (Services)	529
variant	529
version	530
version (Flow Monitoring Logs for NAT)	531
version9 (Forwarding Options)	531
version-ipfix (Services)	532
video-monitoring	533
world-readable	534
Chapter 16	
Operational Commands	535
clear passive-monitoring statistics	537
clear services accounting statistics inline-jflow	538
clear services dynamic-flow-capture	539
clear services flow-collector statistics	540
clear services rpm twamp server connection	541
clear services service-sets statistics jflow-log	542
clear services video-monitoring mdi errors fpc-slot	543
clear services video-monitoring mdi statistics fpc-slot	544
request services flow-collector change-destination primary interface	545
request services flow-collector change-destination secondary interface	546
request services flow-collector test-file-transfer	547
request services rpm twamp	548
show forwarding-options next-hop-group	549
show forwarding-options port-mirroring	552
show interfaces (Dynamic Flow Capture)	554
show interfaces (Flow Collector)	558
show interfaces (Flow Monitoring)	564

show passive-monitoring error	569
show passive-monitoring flow	571
show passive-monitoring memory	573
show passive-monitoring status	575
show passive-monitoring usage	577
show services accounting aggregation	579
show services accounting aggregation template	583
show services accounting errors	584
show services accounting flow	588
show services accounting flow-detail	593
show services accounting memory	598
show services accounting packet-size-distribution	600
show services accounting status	602
show services accounting usage	605
show services dynamic-flow-capture content-destination	607
show services dynamic-flow-capture control-source	609
show services dynamic-flow-capture statistics	611
show services flow-collector file interface	614
show services flow-collector input interface	616
show services flow-collector interface	618
show services rpm active-servers	624
show services rpm history-results	625
show services rpm probe-results	628
show services rpm rfc2544-benchmarking	635
show services rpm rfc2544-benchmarking test-id	640
show services rpm twamp client connection	657
show services rpm twamp client history-results	659
show services rpm twamp client probe-results	663
show services rpm twamp client session	667
show services rpm twamp server connection	669
show services rpm twamp server session	671
show services service-sets statistics jflow-log	673
show services video-monitoring mdi errors fpc-slot	681
show services video-monitoring mdi flows fpc-slot	683
show services video-monitoring mdi stats fpc-slot	687
test services rpm rfc2544-benchmarking test	689

Part 6

Index

Index	693
-----------------	-----

List of Figures

Part 1	Flow Monitoring and Flow Collection Services	
Chapter 1	Monitoring Traffic Using Active Flow Monitoring	3
	Figure 1: Active Monitoring Configuration Topology	5
Chapter 2	Monitoring Traffic Using Passive Flow Monitoring	25
	Figure 2: Passive Monitoring Application Topology	26
Chapter 3	Processing and Exporting Multiple Records Using Flow Collection	35
	Figure 3: Flow Collector Interface Topology Diagram	40
Part 2	Flow Capture Services	
Chapter 5	Dynamically Capturing Packet Flows Using Junos Capture Vision	79
	Figure 4: Junos Capture Vision Topology	80
Chapter 6	Detecting Threats and Intercepting Flows Using Junos Packet Vision	91
	Figure 5: Junos Packet Vision Topology	93
Part 3	Sampling, Discard Accounting, and Port Mirroring Services	
Chapter 7	Sampling Data Using Traffic Sampling and Discard Accounting	103
	Figure 6: Configuring Sampling Rate	106
Chapter 10	Sending Packets for Analysis Using Port Mirroring	173
	Figure 7: Active Flow Monitoring—Multiple Port Mirroring with Next-Hop Groups Topology Diagram	192
Part 4	Real-Time Performance Monitoring and Video Monitoring Services	
Chapter 13	Testing the Performance of Network Devices Using RFC 2544-Based Benchmarking	227
	Figure 8: E-LAN And E-Line Reflection in a metro Solution	231
	Figure 9: RFC 2544-Based Benchmarking Test for a Layer 3 IPv4 Service	240
	Figure 10: RFC 2544-Based Benchmarking Test for UNI Direction of an Ethernet Pseudowire	248
	Figure 11: RFC 2544-Based Benchmarking Test for NNI Direction of an Ethernet Pseudowire	256
	Figure 12: Layer 2 reflection Simple Topology	263
	Figure 13: Layer 2 Reflection with Simple BGP-based VPLS Topology	288

List of Tables

	About the Documentation	xxi
	Table 1: Notice Icons	xxiii
	Table 2: Text and Syntax Conventions	xxiv
Part 1	Flow Monitoring and Flow Collection Services	
Chapter 1	Monitoring Traffic Using Active Flow Monitoring	3
	Table 3: Quick Reference to Key Configuration Statements at This Hierarchy Level	17
	Table 4: Quick Reference to Configuration Statements at This Hierarchy Level	18
	Table 5: Quick Reference to Key Configuration Statements at this Hierarchy Level	18
Chapter 4	Logging Flow Monitoring Records With Version 9 and IPFIX Templates for NAT Events	47
	Table 6: Flow Template Format for NAT44 Session Creation and Deletion	51
	Table 7: Flow Template Format for NAT64 Session Creation and Deletion	51
	Table 8: Flow Template Format for NAT44 BIB Creation and Deletion	52
	Table 9: Flow Template Format for NAT64 BIB Creation and Deletion	52
	Table 10: Flow Template Format for Address Exhausted Events	53
	Table 11: Flow Template Format for Ports Exhausted Events	53
	Table 12: Flow Template Format for NAT44 Quota Exceeded Events	53
	Table 13: Flow Template Format for NAT64 Quota Exceeded Events	54
	Table 14: Flow Template Format for NAT44 Address Binding Creation and Deletion Events	54
	Table 15: Flow Template Format for NAT64 Address Binding Creation and Deletion Events	54
	Table 16: Flow Template Format for NAT44 Port Block Allocation and Deallocation Events	55
	Table 17: Flow Template Format for NAT64 Port Block Allocation and Deallocation Events	55
	Table 18: Association Between natEvent Values and Names	56
Part 3	Sampling, Discard Accounting, and Port Mirroring Services	
Chapter 9	Sampling Data Using Flow Aggregation	131
	Table 19: IPv4 Template Fields	154
	Table 20: IPv6 Template Fields	155
	Table 21: Example of Observation Domain ID	159
	Table 22: Values of Template and Option Template IDs for IPFIX Flows	162

	Table 23: Values of Template and Option Template IDs for Version 9 Flows	162
	Table 24: Values of Template and Option Template IDs for IPFIX Flows	163
	Table 25: Values of IPv6 Options and Extension Headers in Packets	167
Part 4	Real-Time Performance Monitoring and Video Monitoring Services	
Chapter 11	Monitoring Traffic Using Real-Time Performance Monitoring	199
	Table 26: RPM Tracing Flags	217
Chapter 13	Testing the Performance of Network Devices Using RFC 2544-Based Benchmarking	227
	Table 27: Supported Network Topologies for RFC2544 Benchmarking Tests . . .	229
	Table 28: Supported Interfaces for RFC2544 Benchmarking Tests	229
	Table 29: MAC Address Swapping Behavior for E-LAN and E-Line Services . . .	232
	Table 30: Supported RFC2544-Based Benchmarking Reflector Statements on MX104	234
Chapter 14	Tracking Streaming Media Traffic Using Inline Video Monitoring	309
	Table 31: MPC Flow Monitoring Capacity by Model	311
	Table 32: show services video-monitoring mdi stats fpc-slot Output Fields . . .	315
	Table 33: show services video-monitoring mdi errors fpc-slot Output Fields . .	316
	Table 34: show services mdi flows Output Fields	316
Part 5	Configuration Statements and Operational Commands	
Chapter 16	Operational Commands	535
	Table 35: show forwarding-options next-hop-group Output Fields	549
	Table 36: show forwarding-options port-mirroring Output Fields	552
	Table 37: Dynamic Flow Capture show interfaces Output Fields	554
	Table 38: Flow Collector Show interfaces Output Fields	558
	Table 39: show interfaces Output Fields (Flow Monitoring)	564
	Table 40: show passive-monitoring error Output Fields	569
	Table 41: show passive-monitoring flow Output Fields	571
	Table 42: show passive-monitoring memory Output Fields	573
	Table 43: show passive-monitoring status Output Fields	575
	Table 44: show passive-monitoring usage Output Fields	577
	Table 45: show services accounting aggregation Output Fields	580
	Table 46: show services accounting aggregation template Output Fields	583
	Table 47: show services accounting errors Output Fields	584
	Table 48: show services accounting flow Output Fields	588
	Table 49: show services accounting flow-detail Output Fields	594
	Table 50: show services accounting memory Output Fields	598
	Table 51: show services accounting packet-size-distribution Output Fields . .	600
	Table 52: show services accounting status Output Fields	602
	Table 53: show services accounting usage Output Fields	605
	Table 54: show services dynamic-flow-capture content-destination Output Fields	607
	Table 55: show services dynamic-flow-capture control-source Output Fields . .	609
	Table 56: show services dynamic-flow-capture statistics Output Fields	611

Table 57: show services flow-collector file interface Output Fields	614
Table 58: show services flow-collector input interface Output Fields	616
Table 59: show services flow-collector interface Output Fields	618
Table 60: show services rpm active-servers Output Fields	624
Table 61: show services rpm history-results Output Fields	625
Table 62: show services rpm probe-results Output Fields	628
Table 63: show services rpm rfc2544-benchmarking Output Fields	636
Table 64: show services rpm rfc2544-benchmarking test-id Output Fields	641
Table 65: show services rpm twamp client connection Output Fields	657
Table 66: show services rpm twamp client history-results Output Fields	659
Table 67: show services twamp client probe-results Output Fields	663
Table 68: show services rpm twamp client session Output Fields	667
Table 69: show services rpm twamp server connection Output Fields	669
Table 70: show services rpm twamp server session Output Fields	671
Table 71: show services service-sets statistics jflow-log Output Fields	673
Table 72: show services video-monitoring mdi errors fpc-slot Output Fields	681
Table 73: show services mdi flows Output Fields	684
Table 74: show services video-monitoring mdi stats fpc-slot Output Fields	687

About the Documentation

- Documentation and Release Notes on page xxi
- Supported Platforms on page xxi
- Using the Examples in This Manual on page xxi
- Documentation Conventions on page xxiii
- Documentation Feedback on page xxv
- Requesting Technical Support on page xxv

Documentation and Release Notes

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

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

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- M Series
- MX Series
- T Series

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 [CLI Explorer](#).

Documentation Conventions

[Table 1 on page xxiii](#) 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 xxiv](#) defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<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@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(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.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

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

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

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 of the Juniper Networks TechLibrary 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 <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to 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 Partner Support Service support contract, or are covered under warranty, and need post-sales 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/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- 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, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Flow Monitoring and Flow Collection Services

- [Monitoring Traffic Using Active Flow Monitoring on page 3](#)
- [Monitoring Traffic Using Passive Flow Monitoring on page 25](#)
- [Processing and Exporting Multiple Records Using Flow Collection on page 35](#)
- [Logging Flow Monitoring Records With Version 9 and IPFIX Templates for NAT Events on page 47](#)

CHAPTER 1

Monitoring Traffic Using Active Flow Monitoring

- [Active Flow Monitoring Overview on page 3](#)
- [Configuring Flow Monitoring on page 6](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 11](#)
- [Example: Configuring Flow Monitoring on MS-MIC and MS-MPC on page 14](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 21](#)
- [Flow Offloading on page 23](#)

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 11](#) 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:

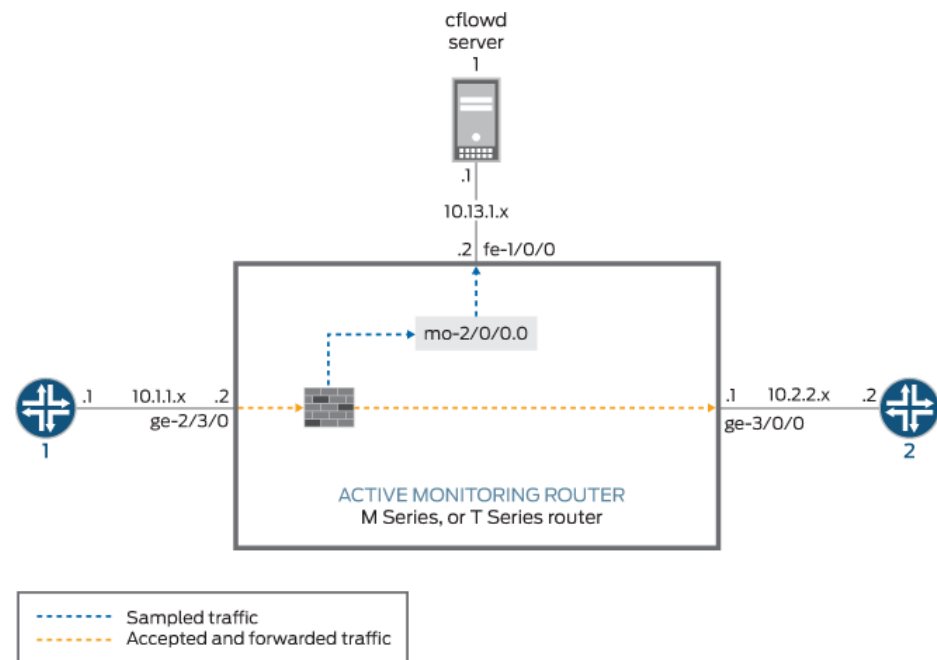
- The router or switch can perform sampling *or* port mirroring at any one time.
- The router or switch can perform forwarding *or* discard accounting at any one time.

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 1 on page 5 shows a sample topology.

Figure 1: Active Monitoring Configuration Topology



In Figure 1 on page 5, 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 6](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 167](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 21](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 11](#)

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 6](#)
- [Configuring Flow-Monitoring Properties on page 8](#)
- [Example: Configuring Flow Monitoring on page 10](#)

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.example.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.



NOTE: Starting with Junos OS Release 15.1, instead of an eJunos kernel core file, the multiservices PIC management daemon core file is generated when a prolonged flow control failure occurs and when you configure the setting to generate a core dump during prolonged flow control (by using the **dump-on-flow-control** option with the **flow-control-options** statement). The watchdog functionality continues to generate a kernel core file in such scenarios.

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 8](#)
- [Exporting Flows on page 9](#)
- [Configuring Time Periods when Flow Monitoring is Active and Inactive on page 9](#)

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.

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 132.

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 15.1*. For information on cflowd, see [“Enabling Flow Aggregation” on page 132](#).

```
[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 3](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 167](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 21](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 11](#)

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;
    version9 {
      template {
        mpls-ls1;
      }
    }
  }
}
}
services {
  flow-monitoring {
    version9 {
      template ipv4-ls1 {
        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-ls1 {
        mpls-template;
      }
    }
  }
}
}

```

- Related Documentation**
- [Active Flow Monitoring Overview on page 3](#)
 - [Configuring Flow Monitoring on page 6](#)

- [Directing Replicated Flows to Multiple Flow Servers on page 167](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 21](#)

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 14](#)
- [Junos Traffic Vision Support on MS-MIC and MS-MPC on page 14](#)
- [Configuring Flow Monitoring on MS-MIC on page 16](#)
- [Verification on page 20](#)

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.



NOTE: When Junos Traffic Vision is configured on the MS-MIC and MS-MPC, the next-hop address and outgoing interfaces are incorrectly displayed in the IPv4 and IPv6 flow records when the destination of the sampled flow is reachable through multiple paths.

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 3: Quick Reference to Key Configuration Statements at This Hierarchy Level

Configuration Statement	Description
flow-active-timeout	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.
flow-inactive-timeout	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.
template-refresh-rate	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.
option-refresh-rate	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 4: Quick Reference to Configuration Statements at This Hierarchy Level

Configuration Statement	Description
sampling	Configures the service set to handle sampling/flow monitoring activities.
service-interface	Specifies the service interface associated with the service set. The interface configured here should match the interface configured at the [edit forwarding-options sampling family inet output] . 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 5: Quick Reference to Key Configuration Statements at this Hierarchy Level

Configuration Statement	Description
rate	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.
run-length	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.
flow-server	A host system to collect sampled flows using the version 9 format.

Table 5: Quick Reference to Key Configuration Statements at this Hierarchy Level (*continued*)

source-address	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 20](#)
- [Viewing the Flow Details on page 20](#)
- [Viewing Details of Errors That Occurred on the Services Interface on page 20](#)

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
```

- Related Documentation**
- *Multiservices MIC and Multiservices MPC (MS-MIC and MS-MPC) Overview*
 - *Example: Configuring Junos VPN Site Secure on MS MIC and MS-MPC*

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*. 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 3](#)
- [Configuring Flow Monitoring on page 6](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 167](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 11](#)

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 526](#)

CHAPTER 2

Monitoring Traffic Using Passive Flow Monitoring

- [Passive Flow Monitoring Overview on page 25](#)
- [Enabling Passive Flow Monitoring on page 26](#)

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).

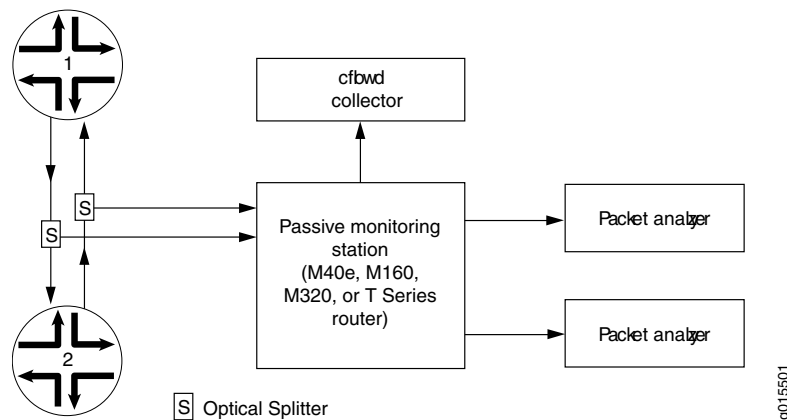


NOTE: Monitoring Services PICs, AS PICs, and Multiservices PICs must be mounted on an Enhanced Flexible PIC Concentrator (FPC) in an M Series or T Series router.

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 2 on page 26](#) shows a typical topology for the passive flow-monitoring application.

Figure 2: 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 26](#)

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 6](#).

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 28](#)
- [Example: Enabling IPv4 Passive Flow Monitoring on page 30](#)
- [Example: Enabling IPv6 Passive Flow Monitoring on page 32](#)

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 *MPLS Applications Feature Guide 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 | gigether-options | sonet-options) mpls]** hierarchy level:

```
[edit interfaces interface-name (atm-options | fastether-options | gigether-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 | gigether-options | sonet-options) mpls pop-all-labels]** hierarchy level:

```
[edit interfaces interface-name (atm-options | fastether-options | gigether-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 25](#)

CHAPTER 3

Processing and Exporting Multiple Records Using Flow Collection

- [Flow Collection Overview on page 35](#)
- [Configuring Flow Collection on page 36](#)
- [Example: Configuring Flow Collection on page 40](#)
- [Sending cflowd Records to Flow Collector Interfaces on page 46](#)
- [Configuring Flow Collection Mode and Interfaces on Services PICs on page 46](#)

Flow Collection Overview

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

Related Documentation

- [Configuring Flow Collection on page 361](#)
- [Sending cflowd Records to Flow Collector Interfaces on page 46](#)
- [Configuring Flow Collection Mode and Interfaces on Services PICs on page 46](#)

Configuring Flow Collection

This section describes the following tasks for configuring flow collection:

- [Configuring Destination FTP Servers for Flow Records on page 36](#)
- [Configuring a Packet Analyzer on page 37](#)
- [Configuring File Formats on page 37](#)
- [Configuring Interface Mappings on page 38](#)
- [Configuring Transfer Logs on page 38](#)
- [Configuring Retry Attempts on page 39](#)

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.

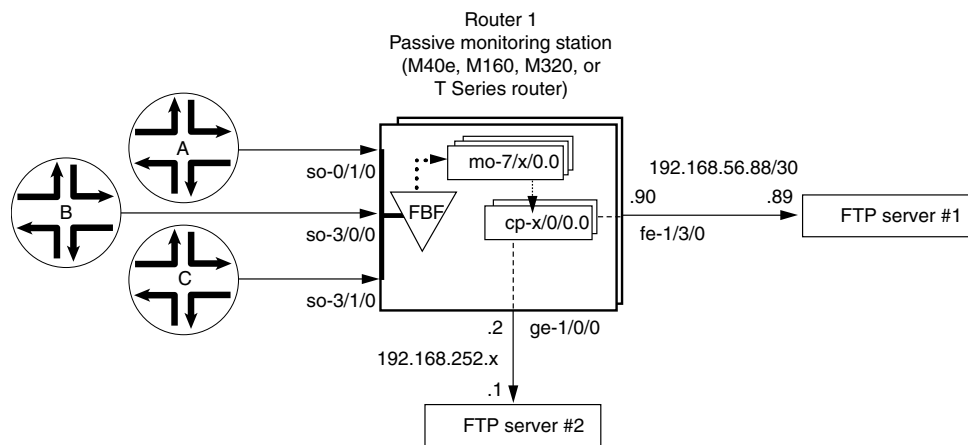
Related Documentation

- [Flow Collection Overview on page 35](#)
- [Sending cflowd Records to Flow Collector Interfaces on page 46](#)
- [Configuring Flow Collection Mode and Interfaces on Services PICs on page 46](#)
- [Example: Configuring Flow Collection on page 40](#)

Example: Configuring Flow Collection

Figure 3 on page 40 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 3: Flow Collector Interface Topology Diagram



- Monitored traffic is converted into cflowd records by the Monitoring Services interfaces
- cflowd records are delivered to the flow collector interfaces
- Processed files are sent from the flow collector interfaces to the FTP servers

g003250

```
[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 "$ABC123"; # SECRET-DATA
  }
  "ftp://user@192.168.252.1//tmp/collect2/" { # The secondary FTP server.
    password "$ABC123"; # SECRET-DATA
  }
}
file-specification { # Define sets of flow collector characteristics here.
  def-spec {
    name-format "default-allInt-0-%D_%T-%I_%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-%I_%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 "$ABC123";
    }
  }
}
}
}
}

```

Related Documentation

- [Flow Collection Overview on page 35](#)
- [Configuring Flow Collection on page 36](#)
- [Sending cflowd Records to Flow Collector Interfaces on page 46](#)
- [Configuring Flow Collection Mode and Interfaces on Services PICs on page 46](#)

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 on page 35](#)
- [Configuring Flow Collection on page 36](#)
- [Configuring Flow Collection Mode and Interfaces on Services PICs on page 46](#)
- [Example: Configuring Flow Collection on page 40](#)

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 on page 35](#)
- [Configuring Flow Collection on page 36](#)
- [Sending cflowd Records to Flow Collector Interfaces on page 46](#)
- [Example: Configuring Flow Collection on page 40](#)

CHAPTER 4

Logging Flow Monitoring Records With Version 9 and IPFIX Templates for NAT Events

- [Logging NAT Events in Flow Monitoring Format Overview on page 48](#)
- [Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57](#)
- [Exporting Syslog Messages to an External Host Without Flow Monitoring Formats Overview on page 58](#)
- [Exporting Version 9 Flow Data Records to a Log Collector Overview on page 59](#)
- [Exporting IPFIX Flow Data Records to a Log Collector Overview on page 60](#)
- [Mapping Between Field Values for Version 9 Flow Templates and Logs Exported on page 61](#)
- [Mapping Between Field Values for IPFIX Flow Templates and Logs Exported on page 64](#)
- [Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68](#)
- [Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69](#)

Logging NAT Events in Flow Monitoring Format Overview

Starting with Junos OS Release 14.2R2 and 15.1R1, you can configure MX Series routers with MS-MPCs and MS-MICs to log network address translation (NAT) events using the Junos Traffic Vision (previously known as Jflow) version 9 or IPFIX (version 10) template format. NAT event logger generates messages in flow monitoring format for various NAT events, such as the creation of a NAT entry, deletion of a NAT entry, and for invalid NAT processing (such as NAT address pools or address values being exhausted for allocation). These events also support NAT64 translations (translation of IPv6 addresses to IPv4 addresses), binding information base (BIB) events, and more detailed error generation. The generated records or logs for NAT events in flow template format are sent from the MS-MIC or MS-MPC to the specified host or external device that functions as the NetFlow collector. This method of generating flow monitoring records for NAT events enables cohesive and streamlined analysis of NAT traffic and troubleshooting of NAT-related problems. You can enable the capability to send flow monitoring records for NAT operations to an external collector and the capability to use the system logging protocol (syslog) to generate session logging for different services at the same time.

The flow records and the templates are encapsulated in an UDP or IP packet and sent to the collector. However, TCP-based logging of monitoring records for NAT events is not supported. Carrier-grade NAT (CGN) devices are required to log events creation and deletion of translations and information about the resources it manages. Flow monitoring logs can be optionally configured in your network topology in addition to the system logging (syslog) capability, which causes logs to be saved from the PIC to either the in the `/var/log` directory of the Routing Engine (local) or to an external server (remote). Generally, flow collectors are the part of a vast network infrastructure containing several third-party devices, which perform various correlations and mappings with logs of other databases. Therefore, collection of NAT-related flow monitoring records as logs or template records is useful on the hosts or devices that function as collectors in an overall and comprehensive perspective. You can enable logging of flow monitoring records for NAT events at the service-set level to enable version 9 or IPFIX flow records to be generated as logs when NAT is configured on the router.

The NetFlow collector receives flow records in version 9 or IPFIX format from one or more exporters. It processes the received export packets by parsing and saving the flow record details. Flow records can be optionally aggregated before being stored on the hard disk. The NetFlow collector is also referred to as the collector. The exporter monitors packets entering an observation point and creates flows from these packets. The information from these flows is exported in the form of flow records to the NetFlow Collector. An observation point is a location in the network where IP packets can be overseen and monitored; for example, one or a set of interfaces on a network device such as a router. Every observation point is associated with an observation domain, which is a cluster of observation points, and constitutes the largest aggregatable set of flow information at the network device with NetFlow services enabled.

A FlowSet is a generic term for a collection of Flow Records that have a similar pattern or format. In an export packet, one or more FlowSets follow the packet header. A Template FlowSet comprises one or more template records that have been grouped together in an export packet. An Options Template FlowSet contains one or more Options Template

records that are combined together in an export packet. A Data FlowSet is one or more records, of the same type, that are grouped together in an export packet. Each record is either a flow data record or an options data record that has been previously specified by a Template Record or an Options Template Record. One of the essential elements in the NetFlow format is the Template FlowSet. Templates vastly enhance the flexibility of the Flow Record format because they allow the collector to process Flow Records without necessarily knowing the interpretation of all the data in the Flow Record.

You can configure the capability to transmit records or log messages in version 9 and IPFIX traffic flow formats generated for NAT events to an external, off-box high-speed NetFlow collector for easy and effective monitoring and diagnosis of the logs. By default, this functionality is disabled. With a high number of NAT events, this mechanism of exporting logs to an external log collector might cause scaling considerations such as loss of a few flow records. To enable the mechanism to record logging messages in flow monitoring format for NAT events, you can now include the **jflow-log** statement at the **[edit services]** hierarchy level. You can configure a collector, which is an external host to which the flow monitoring formatted logs are sent, or a group of collectors. A group of collectors is useful in scenarios in which you want to combine a set of collector devices and define common settings for logging NAT events for all the collectors in the cluster or group.

To configure a collector and its parameters, such as the source IP address from which the records are sent and the destination address of the collector, include the **collector collector-name** statement and its substatements at the **[edit services jflow-log]** hierarchy level. To specify a collector group or a cluster, include the **collector-group collector-group-name** statement and its substatements at the **[edit services jflow-log]** hierarchy level.

You need to configure a template profile and associate it with the collector. The profile defines the characteristics of the flow monitoring record template, such as the version of flow monitoring (version 9 or IPFIX), the refresh rate, in either packets or seconds, and the type of service or application (NAT in this case) for which flow records must be sent to the collector. To specify a template profile, include the **template-profile template-profile-name** statement at the **[edit services jflow-log]** hierarchy level. To specify the maximum number of messages to be collected per second for NAT error events, include the **message-rate-limit messages-per-second** statement at the **[edit interfaces ms-interface-name service-options jflow-log]** hierarchy level.

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. You must define a template profile properties for a NAT service and associate the defined template profile with a service set to enable the flow monitoring log functionality for NAT events. To define the template profile characteristics for recording flow monitoring logs for NAT events, include the **template-profile template-profile-name** statement at the **[edit services jflow-log]** hierarchy level. To associate the template profile for recording flow monitoring logs for NAT events with a service-set level, which applies for all the services in the system, include the **template-profile template-profile-name** statement at the **[edit services service-set service-set-name]** hierarchy level.

To view statistical information on the logs generated in flow monitoring format for the interfaces and service sets configured on the system, use the **show services service-sets statistics jflow-log** command.

The following system log messages for various NAT events are logged using the system logging (syslog) capability:

- JSERVICES_SESSION_OPEN
- JSERVICES_SESSION_CLOSE
- JSERVICES_NAT_OUTOF_ADDRESSES
- JSERVICES_NAT_OUTOF_PORTS
- JSERVICES_NAT_RULE_MATCH
- JSERVICES_NAT_POOL_RELEASE
- JSERVICES_NAT_PORT_BLOCK_ALLOC
- JSERVICES_NAT_PORT_BLOCK_RELEASE
- JSERVICES_NAT_PORT_BLOCK_ACTIVE

The following NAT events are logged using the flow monitoring log capability using version 9 and IPFIX flow templates:

- NAT44 session create
- NAT44 session delete
- NAT addresses exhausted
- NAT64 session create
- NAT64 session delete
- NAT44 BIB create
- NAT44 BIB delete
- NAT64 BIB create
- NAT64 BIB delete
- NAT ports exhausted
- NAT quota exceeded
- NAT Address binding create
- NAT Address binding delete
- NAT port block allocation
- NAT port block release
- NAT port block active

[Table 6 on page 51](#) describes the flow template format for NAT44 session creation and deletion events. The Information Element (IE) names and their IANA IDs are as defined

in the IP Flow Information Export (IPFIX) Entities specification by the Internet Assigned Numbering Authority (IANA).

Table 6: Flow Template Format for NAT44 Session Creation and Deletion

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
sourceIPv4Address	32	8
postNATSourceIPv4Address	32	225
protocolIdentifier	8	4
sourceTransportPort	16	7
postNAPTsourceTransportPort	16	227
destinationIPv4Address	32	12
postNATDestinationIPv4Address	32	226
destinationTransportPort	16	11
postNAPTdestinationTransportPort	16	228
natOriginatingAddressRealm	8	229
natEvent	8	230

[Table 7 on page 51](#) describes the flow template format for NAT64 session creation and deletion events.

Table 7: Flow Template Format for NAT64 Session Creation and Deletion

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
sourceIPv6Address	128	27
postNATSourceIPv6Address	32	225
protocolIdentifier	8	4
sourceTransportPort	16	7
postNAPTsourceTransportPort	16	227
destinationIPv6Address	128	28

Table 7: Flow Template Format for NAT64 Session Creation and Deletion (*continued*)

Information Element (IE)	Size (bits)	IANA ID
postNATDestinationIPv6Address	32	226
destinationTransportPort	16	11
postNAPTdestinationTransportPort	16	228
natOriginatingAddressRealm	8	229
natEvent	8	230

[Table 8 on page 52](#) describes the flow template format for NAT44 binding information base (BIB) creation and deletion events.

Table 8: Flow Template Format for NAT44 BIB Creation and Deletion

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
sourceIPv4Address	32	8
postNATSourceIPv4Address	32	225
protocolIdentifier	8	4
sourceTransportPort	16	7
postNAPTsourceTransportPort	16	227
natEvent	8	230

[Table 9 on page 52](#) describes the flow template format for NAT64 binding information base (BIB) creation and deletion events.

Table 9: Flow Template Format for NAT64 BIB Creation and Deletion

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
sourceIPv6Address	128	27
postNATSourceIPv6Address	32	225
protocolIdentifier	8	4

Table 9: Flow Template Format for NAT64 BIB Creation and Deletion (*continued*)

Information Element (IE)	Size (bits)	IANA ID
sourceTransportPort	16	7
postNAPTsourceTransportPort	16	227
natEvent	8	230

[Table 10 on page 53](#) describes the flow template format for addresses exhaustion events.

Table 10: Flow Template Format for Address Exhausted Events

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
natEvent	8	230
natPoolName	512	284

[Table 11 on page 53](#) describes the flow template format for ports exhaustion events.

Table 11: Flow Template Format for Ports Exhausted Events

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
natEvent	8	230
postNATSourceIPv4Address	32	225
protocolIdentifier	8	4

[Table 12 on page 53](#) describes the flow template format for NAT44 quota exceeded events.

Table 12: Flow Template Format for NAT44 Quota Exceeded Events

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
natEvent	8	230
sourceIPv4Address	32	8

[Table 13 on page 54](#) describes the flow template format for NAT64 quota exceeded events.

Table 13: Flow Template Format for NAT64 Quota Exceeded Events

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
natEvent	8	230
sourceIPv6Address	128	27

[Table 14 on page 54](#) describes the flow template format for NAT44 address binding creation and deletion events.

Table 14: Flow Template Format for NAT44 Address Binding Creation and Deletion Events

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
natEvent	8	230
sourceIPv4Address	32	8
postNATSourceIPv4Address	32	225

[Table 15 on page 54](#) describes the flow template format for NAT64 address binding creation and deletion events.

Table 15: Flow Template Format for NAT64 Address Binding Creation and Deletion Events

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
natEvent	8	230
sourceIPv6Address	128	27
postNATSourceIPv4Address	32	225

[Table 16 on page 55](#) describes the flow template format for NAT44 port block allocation and deallocation events.

Table 16: Flow Template Format for NAT44 Port Block Allocation and Deallocation Events

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
sourceIPv4Address	32	8
postNATSourceIPv4Address	32	225
portRangeStart	16	361
portRangeEnd	16	362
portRangeStepSize	16	363
portRangeNumPorts	16	364
observationTimeMilliseconds (time when PBA allocated)	64	323
natEvent	8	230

[Table 17 on page 55](#) describes the flow template format for NAT64 port block allocation and deallocation events.

Table 17: Flow Template Format for NAT64 Port Block Allocation and Deallocation Events

Information Element (IE)	Size (bits)	IANA ID
observationTimeMilliseconds	64	323
sourceIPv6Address	128	27
postNATSourceIPv4Address	32	225
portRangeStart	16	361
portRangeEnd	16	362
portRangeStepSize	16	363
portRangeNumPorts	16	364
observationTimeMilliseconds (time when port block allocation (PBA) is configured)	64	323
natEvent	8	230

In all of the aforementioned templates, the `natEvent` field maps to one of the values listed in [Table 18 on page 56](#), depending on the type of event.

Table 18: Association Between `natEvent` Values and Names

natEvent Value	natEvent Name
1	NAT44 Session create
2	NAT44 Session delete
3	NAT Addresses exhausted
4	NAT64 Session create
5	NAT64 Session delete
6	NAT44 BIB create
7	NAT44 BIB delete
8	NAT64 BIB create
9	NAT64 BIB delete
10	NAT ports exhausted
11	NAT Quota exceeded
12	NAT Address binding create
13	NAT Address binding delete
14	NAT port block allocation
15	NAT port block release
16	NAT port block active

Related Documentation

- [Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57](#)
- [Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68](#)
- [Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69](#)

Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format

Keep the following points in mind when you configure the capability to generate logs or records in flow monitoring format for NAT events:

- Enabling syslog and Jflow capabilities at the same time might result in scaling impacts because both these mechanisms use a separate infrastructure to transfer records out to the collector.
- High number of NAT events can cause scalability considerations because of the flow monitoring framework too requiring system processes.
- The flow monitoring log infrastructure uses data CPUs to send the logs to the external flow server, which might cause a slight impact on performance.
- An explicit, separate maximum limit on the number of flow monitoring messages that are generated for NAT error events is implemented. You can control the maximum number of NAT error events for which logs in flow monitoring format must be recorded by including the **message-rate-limit messages-per-second** option at the **[edit interfaces interface-name services-options jflow-log]** hierarchy level. These records for NAT error events are generated when addresses for allocation from the NAT pool are not available, when ports for allocation to a subscriber are not available, or when the allocated quota is exceeded for NAT events (more than the configured number of ports is requested). Also, you can configure the **message-rate-limit** option that previously existed at the **[edit interfaces interface-name services-options syslog]** hierarchy level to specify the maximum number of system log messages per second that can be sent from the PIC to either the Routing Engine (local) or to an external server (remote).
- NAT error events such as “Out of Ports”, “Out of Addresses”, and “Quota Exceeded” are rate limited. The default rate limit is 10,000 events per second. This setting is also configurable at PIC level.
- The template for NAT event logging is in accordance with IETF as *IPFIX Information Elements for logging NAT Events—draft-ietf-behave-ipfix-nat-logging-02*.
- Only UDP-based logging is supported, which is an unreliable protocol.
- This functionality is supported on MX Series routers with Junos OS Extension-Provider packages installed and configured on the device, and on MS-MPCs and MS-PICs. It is not supported on MS-DPCs with MX Series routers.
- Transmission of logs occurs in clear-text format similar to other log messages that the services PICs do not encrypt. It is assumed that the transport of logs and the positioning of the log collector are within a secured realm. Because the messages do not contain sensitive details such as username or passwords, the messages do not cause any security or reliability risks.
- Template IDs 0 through 255 are reserved for template sets and the maximum number of templates supported for logging events in flow monitoring format is 255. When you modify a template-profile configuration (changes to the collector or version, or a deactivation and activation of the service set associated with the template), the specific template is deregistered and reregistered. However, the flow monitoring infrastructure

requires 10 minutes by default as the delay period for the template IDs to be freed up. As a result, if you modify the template-profile settings many times within the 10-minute period, the maximum limit on the template IDs of 255 is exceeded and further templates are not registered.

In such a case, when templates are not being registered, you must wait until the delay period for deleting a deregistered template of 10 minutes before you perform any more configuration changes to have templates registered with the flow monitoring application. To examine whether a template has been registered, you can use the **show services service-sets statistics jflow-log** command. If the Sent field displays a non-zero value for template records, it denotes that templates are successfully registered.

- In a scenario in which the capability to log NAT events in flow monitoring format is enabled at the service-set level, and if the PIC boots up, the flow monitoring log templates are registered with the flow monitoring application. During the registration process, a first set of 12 template records are sent to the collector. However, all of the template records might not reach the collector from the PIC on the router or might not be transmitted out of the router because the interface might not be up from the perspective of the Packet Forwarding Engine. After the refresh time of a template expires, next set of template records are sent out to the collector. For example, if the template refresh time is 60 seconds, only after 60 seconds from the time of booting of the PIC, template records are properly sent to the collector.
- If no problems occur in the transmission of flow monitoring log messages to the collector from the PIC, the Sent field is incremented to indicate NAT events being logged for every event. Also, the tcpdump utility at the destination IP address of the collector denotes the reception of UDP packets. If NAT processing occurs and the value in the **Dropped** section of the output of the **show services service-sets statistics jflow-log service-set service-set-name** command is incremented or not incremented, you must examine the debugging statistics and counters to determine if any problems exist in the network for transmission of the flow monitoring log messages.

Related Documentation

- [Logging NAT Events in Flow Monitoring Format Overview on page 48](#)
- [Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68](#)
- [Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69](#)

Exporting Syslog Messages to an External Host Without Flow Monitoring Formats Overview

Until Junos OS Release 14.2R1, the only mechanism you could use to generate logs for NAT sessions was by enabling system logging for service sets and transferring syslog messages to either the internal local host on the Routing Engine or to an external host server. When a syslog is enabled with the class or component being NAT logs and session logs configured, NAT events are recorded. A sample of one such syslog output is as follows:

```
{service_set_3}[jservices-nat]: JSERVICES_NAT_RULE_MATCH: proto 17(UDP) app: any,
xe-3/1/1.0#012 24.0.0.2/18575 -> 23.0.0.2/63,Match NAT rule-set (null) rule
```

```

nat-basic_1
term t1
{service_set_3}MSVCS_LOG_SESSION_OPEN: App:none, xe-3/1/1.0#012 24.0.0.2:18575
[31.0.0.17:1048] -> 23.0.0.2:63 (UDP)
{service_set_3}MSVCS_LOG_SESSION_CLOSE: App:none, xe-3/1/1.0#012 24.0.0.2:18575
[31.0.0.17:1048] -> 23.0.0.2:63 (UDP)

```

From the preceding syslog output, it denotes that NAT create log (NAT translation) and delete log (NAT release) are generated during session events as a part of session-logs configuration. Another important log that is NAT pool exhaustion (not illustrated in the preceding example) is generated as a part of NAT-logs configuration. Such an event message might be caused by Address pooling paired (APP), endpoint-independent mapping (EIM), or address and port exhaustion.

Exporting Version 9 Flow Data Records to a Log Collector Overview

A flow record template defines a collection of fields with corresponding descriptions of the format and syntax for the elements or attributes that are contained in it. Network elements (such as routers and switches), which are called exports, accumulate the flow data and export the information to collectors, which are hosts or external devices that can save a large volume of such system log messages for events or system operations. The collected data provides granular, finer-level metering and statistical data for highly flexible and detailed resource usage accounting. Templates that are sent to the collector contain the structural information about the exported flow record fields; therefore, if the collector cannot interpret the formats of the new fields, it can still process the flow record.

The version 9 flow template has a predefined format. An export packet consists of a packet header followed by one or more FlowSet fields. The FlowSet fields can be any of the possible three types—Template, Data, or Options Template. The template flowset describes the fields that will be in the data flowsets (or flow records). Each data flowset contains the values or statistics of one or more flows with the same template ID. An interleaved NetFlow version 9 export packet contains the packet header, Template FlowSet, and Data FlowSet fields. A Template FlowSet field signifies each event such as the creation of a NAT entry or the release of a NAT entry allocated, and the Data FlowSet field denotes the NAT sessions for which the Template FlowSet (or the event type) is associated. For example, if a NAT address entry creation, exhaustion of addresses in a NAT pool, and a NAT entry deletion or release occur, an interleaved version 9 export packet contains the packet header, one Template FlowSet field for NAT address creation, two Data FlowSet fields for the two sessions for which address creation is performed, another TemplateSet field for NAT address deletion, two Data FlowSet fields for the two sessions for which address deletion event occurs, and the other TemplateSet field for NAT pool consumption having exceeded the configured number of pools.

The following are the possible combinations that can occur in an export packet:

- An export packet that consists of interleaved template and data FlowSets—A collector device should not assume that the template IDs defined in such a packet have any specific relationship to the data FlowSets within the same packet. The collector must always cache any received templates, and examine the template cache to determine the appropriate template ID to interpret a data record.

- An export packet consisting entirely of data FlowSets—After the appropriate template IDs have been defined and transmitted to the collector device, most of the export packets will consist solely of data FlowSets.
- An export packet consisting entirely of template FlowSets—Although this case is the exception, it is possible to receive packets containing only template records. Ordinarily, templates are appended to data FlowSets. However, in some instances only templates are sent. When a router first boots up or reboots, it attempts to synchronize with the collector device as quickly as possible. The router may send template FlowSets at an accelerated rate so that the collector device has sufficient information to parse any subsequent data FlowSets. Also, template records have a limited lifetime, and they must be periodically refreshed. If the refresh interval for a template occurs and no appropriate data FlowSet that needs to be sent to the collector device is present, an export packet consisting only of template FlowSets is sent.

Exporting IPFIX Flow Data Records to a Log Collector Overview

The IPFIX protocol enables you to access IP flow information. The IPFIX collection process receives the flow information traversing through multiple network elements within the data network in a consistent, identical manner of representation and communication of traffic flows from the network elements to the collection point. An IPFIX device hosts at least one exporting process, which transmits flow records to collecting processes. A collector is a device that performs the collecting processes and an exporter is a device that performs the transfer to data to a collector. An IPFIX message consists of a message header followed by one or more Sets. The Sets can be any of the possible three types: Data Set, Template Set, or Options Template Set. Flow monitoring version 10 (IPFIX) message formats are very similar to version 9 message patterns.

The message header contains the following fields:

- Version—Version of the flow record format exported in this message. The value of this field is 0x000a.
- Length—Total length of the IPFIX message, measured in octets, including the header and Sets fields.
- Export Time—Time, in seconds, since midnight Coordinated Universal Time (UTC) of January 1, 1970, at which the IPFIX message header leaves the exporter.
- Sequence Number—Incremental sequence counter with a value of 2^{32} (2 raised to the power of 32) of all IPFIX data records sent from the current Observation Domain by the exporting process. Template and Options Template records do not increase the Sequence Number attribute.
- Observation Domain ID—A 32-bit identifier of the Observation Domain that is locally unique to the exporter.

One of the essential elements in the IPFIX record format is the Template FlowSet record. Templates vastly enhance the flexibility of the Flow Record format because they allow the collector to process Flow Records without necessarily knowing the interpretation of all the data in the Flow Record. A Template Record contains any combination of Internet

Assigned Numbers Authority (IANA)-assigned and/or enterprise-specific information element identifiers.

The format of the Template Record signifies a template record header and one or more Field Specifier attributes. The Template FlowSet record contains the following fields:

- **Enterprise bit**—This is the first bit of the Field Specifier. If this bit is zero, the Information Element Identifier identifies an IETF-specified Information Element, and the four-octet Enterprise Number field must not be present. If this bit is one, the Information Element identifier identifies an enterprise-specific Information Element, and the Enterprise Number field must be present.
- **Information Element identifier**—An Information Element is a protocol and encoding-independent description of an attribute that may appear in an IPFIX Record. It is a numeric value that represents the type of Information Element.
- **Field Length**—Length of the corresponding encoded Information Element, in octets. The value 65535 is reserved for variable-length Information Elements.
- **Enterprise Number**—IANA enterprise number of the authority defining the Information Element identifier in this Template Record.

The Data Records are sent in Data Sets. The Data Record field consists only of a Set Header and one or more Field Values. The Template ID to which the Field Values belong is encoded in the Set Header field "Set ID" ("Set ID" = "Template ID"). Interpretation of the Data Record format can be done only if the Template Record corresponding to the Template ID is available at the collecting procedure. Field Values do not necessarily have a length of 16 bits and are encoded according to their data type specified.

Mapping Between Field Values for Version 9 Flow Templates and Logs Exported

The following table describes different field IDs or values for flow monitoring logs generated for NAT events in version 9 flow record formats and the events that correspond to the field values:

Field ID	Name	Size (Bytes)	Description
8	ipv4 src address	4	IPv4 source address
225	natInsideGlobalAddress	4	It reports a modified value caused by a NAT middlebox (forwarding class and loss priority) represents function after the packet passed the Observation Point.
12	ipv4 destination address	4	IPv4 destination address
226	natOutsideGlobalAddress	4	It reports a modified value caused by a NAT middlebox function after the packet passed the Observation Point.
7	transport source-port	2	TCP/UDP source port

Field ID	Name	Size (Bytes)	Description
227	postNAPTSourceTransportPort	2	It reports a modified value caused by a Network Address Port Translation (NAPT) middlebox function after the packet passed the Observation Point.
11	transport destination-port	2	TCP/UDP destination port
228	postNAPTDestinationTransportPort	2	It reports a modified value caused by a Network Address Port Translation (NAPT) middlebox function after the packet passed the Observation Point.
234	ingressVRFID	4	Unique identifier of the VRF name where the packets of this flow are being received. This identifier is unique per Metering Process.
235	egressVRFID	4	Unique identifier of the VRF name where the packets of this flow are being sent. This identifier is unique per Metering Process.
4	Ip protocol	1	IP protocol byte
229	natOriginatingAddressRealm	1	Indicates whether the session was created because traffic originated in the private or public address realm. postNATSourceIPv4Address, postNATDestinationIPv4Address, postNAPTSourceTransportPort, and postNAPTDestinationTransportPort are qualified with the address realm in perspective. The allowed values are: Private: 1 Public: 2
230	natEvent	1	Indicates a NAT event. The allowed values are: 1 - Create event. 2 - Delete event. 3 - Pool exhausted. A Create event is generated when a NAT translation is created, whether dynamically or statically. A Delete event is generated when a NAT translation is deleted.
1	inBytes	N	Incoming counter with length N x 8 bits for the number of bytes associated with an IP Flow. By default N is 4
2	inPkts	N	Incoming counter with length N x 8 bits for the number of packets associated with an IP Flow. By default N is 4

Field ID	Name	Size (Bytes)	Description
323	observationTimeMilliseconds	8	Specifies the absolute time in milliseconds of an observation that represents a time value in units of milliseconds based on coordinated universal time (UTC). The choice of an epoch, for example, 00:00 UTC, January 1, 1970, is left to corresponding encoding specifications for this type. Leap seconds are excluded. Note that transformation of values might be required between different encodings if different epoch values are used.
27	sourceIPv6Address	16	IPv6 source address
284	natPoolName	64	NAT resource pool name
361	portRangeStart	2	The port number identifying the start of a range of ports. A value of zero indicates that the range start is not specified, ie the range is defined in some other way.
362	portRangeEnd	2	The port number identifying the end of a range of ports. A value of zero indicates that the range end is not specified, and the range is defined in some other way.
363	portRangeStepSize	2	The step size in a port range. The default step size is 1, which indicates contiguous ports. A value of zero indicates that the step size is not specified, and the range is defined in some other way.
364	portRangeNumPorts	2	The number of ports in a port range. A value of zero indicates that the number of ports is not specified, and the range is defined in some other way.

Consider a sample scenario of a NAT address creation event. Based on the fields in the preceding table, for translations that are not available (such as natOutsideGlobalAddress) is set to 0. Ingress and Egress VRF of the flow can be made available. Also, natEvent is equal to 1 (create). The inBytes field is assumed to be 0 or number of bytes of the incoming packet and the inPkts field is either 0 or 1 because it is the first packet into the system when translation happens. The observationTimeMilliseconds field denotes the time when this address translation creation is recorded.

For a NAT address deletion event, for translations that are not available (such as `natOutsideGlobalAddress`) is set to 0. Ingress and Egress VRF of the flow can be made available. Also, `natEvent` is equal to 2 (create). The `inBytes` field denotes the number of bytes for this flow in both the forward or upward, the value of the `inPkts` field denotes the number of packets for this flow in both the upward and backward directions. `observationTimeMilliseconds` is the time when this deletion of translation is recorded.

When the NAT pool is exhausted and no further addresses are remaining for allocation, for translations that are not available (such as `natOutsideGlobalAddress`) is set to 0. Ingress and Egress VRF of the flow can be made available. Also, the `natEvent` field is set to 3 (Pool exhausted). All resource failures are combined as a single event. The `inBytes` field is assumed to be 0 or number of bytes of the incoming packet and the `inPkts` field is either 0 or 1 because it is the first packet into the system when translation happens. The value of the `observationTimeMilliseconds` field is the time when this failed translation is recorded.

Mapping Between Field Values for IPFIX Flow Templates and Logs Exported

A new proposed draft defining IPFIX IEs for logging various NAT events is available in IETF as *IPFIX Information Elements for logging NAT Events—draft-ietf-behave-ipfix-nat-logging-02*. The flow monitoring template format for flow monitoring logs generated for NAT events comply with the templates defined in this draft for logging NAT44/NAT64 session create/delete, binding information base (BIB) create/delete, address exhaust, pool exhaustion, quota exceeded, address binding create/delete, port block allocation and de-allocation events. Also, this draft has an extension for NAT64. Support is implemented for logging events for both NAT44 and NAT64. Apart from those templates defined in this draft, no new user-defined templates are created for logging any NAT events.

The following table lists the extensions to the NAT events. The data record contains the corresponding `natEvent` value to identify the event that is being logged.

Event Name	Values
NAT44 Session create	1
NAT44 Session delete	2
NAT Addresses exhausted	3
NAT64 Session create	4
NAT64 Session delete	5
NAT44 BIB create	6
NAT44 BIB delete	7
NAT64 BIB create	8

Event Name	Values
NAT64 BIB delete	9
NAT ports exhausted	10
Quota exceeded	11
Address binding create	12
Address binding delete	13
Port block allocation	14
Port block deallocation	15

The following table describes the field IDs or values and the corresponding names for IPv6 addresses for IPFIX flows:

Field ID	Name	Size (Bytes)	Description
27	sourceIPv6Address	16	IPv6 source address
28	destinationIPv6Address	16	IPv6 destination address
281	postNATSourceIPv6Address	16	Translated source IPv6 address
282	postNATDestinationPv6Address	16	Translated destination IPv6 address

The following table describes the field names and whether they are required or not for NAT64 session creation and deletion events:

Field Name	Size (Bytes)	Whether the Field Is Mandatory
timeStamp	64	Yes
vlanID/ingressVRFID	32	No
sourceIPv4Address	128	Yes
postNATSourceIPv4Address	32	Yes
protocolIdentifier	8	Yes
sourceTransportPort	16	Yes
postNAPTsourceTransportPort	16	Yes

Field Name	Size (Bytes)	Whether the Field Is Mandatory
destinationIPv4Address	128	No
postNATDestinationIPv4Address	32	No
destinationTransportPort	16	No
postNAPTdestinationTransportPort	16	No
natOriginatingAddressRealm	8	No
natEvent	8	Yes

A NAT44 session creation template record can contain the following fields. The natEvent field contains a value of 1, which indicates a NAT44 session creation event. An example of such a template is as follows:

Field Name	Size (Bytes)	Value
timeStamp	64	09:20:10:789
sourceIPv4Address	32	192.168.16.1
postNATSourceIPv4Address	32	201.1.1.100
protocolIdentifier	8	TC
sourceTransportPort	16	14800
postNAPTsourceTransportPort	16	1024
destinationIPv4Address	32	207.85.231.104
postNATDestinationIPv4Address	32	207.85.231.104
destinationTransportPort	16	80
postNAPTdestinationTransportPort	16	80
natOriginatingAddressRealm	8	0
natEvent	8	1

A NAT44 session deletion template record can contain the following fields. The natEvent field contains a value of 2, which indicates a NAT44 session deletion event. An example of such a template is as follows:

Field Name	Size (Bytes)	Value
timeStamp	64	09:20:10:789
sourceIPv4Address	32	192.168.16.1
postNATSourceIPv4Address	32	201.1.1.100
protocolIdentifier	8	TC
sourceTransportPort	16	14800
postNAPTsourceTransportPort	16	1024
destinationIPv4Address	32	207.85.231.104
postNATDestinationIPv4Address	32	207.85.231.104
destinationTransportPort	16	80
postNAPTdestinationTransportPort	16	80
natOriginatingAddressRealm	8	0
natEvent	8	2

Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats

You can configure MX Series routers with MS-MPCs and MS-MICs to log network address translation (NAT) events using the Junos Traffic Vision (previously known as Jflow) version 9 or IPFIX (version 10) template format. NAT event logger generates logs or template records in flow monitoring format and transmits them to the specified external collector or server for various NAT events, such as NAT44 and NAT64 session creation and deletion, and NAT44 and NAT64 binding information base events.



NOTE: This functionality is supported on MX Series routers with Junos OS Extension-Provider packages installed and configured on the device, and on MS-MPCs and MS-PICs. It is not supported on MS-DPCs with MX Series routers.

You can configure the mechanism to record logging messages in flow monitoring format for NAT events. You need to define collectors, and template profiles that contain the properties for flow monitoring logs. You can create a template profile for a particular NAT service on an MX Series router with MS-MPCs or MS-MICs, or for a service set, which applies for all of the NAT services. You can define a template profile to generate flow monitoring logs in a specific flow template format and associate the specified template profile with a service set.

To enable the flow monitoring log capability for NAT events and configure the transmission of logs to collectors at a service level:

1. Define the flow monitoring log service to be applied on an interface to control the maximum number of flow monitoring logs generated for NAT error events.

```
[edit]
user@host# set interfaces ms-fpc/pic/port services-options jflow-log
message-rate-limit messages-per-second
```

For example:

```
[edit]
user@host# set interfaces ms-5/0/0 services-options jflow-log message-rate-limit
50
```

2. Configure the collectors and collector groups.

```
[edit]
user@host# set services jflow-log collector collector-name destination-address address
destination-port port-number source-ip address
user@host# set services jflow-log collector-group collector-group-name collector [
collector-name1 collector-name2]
```

For example:

```
[edit]
user@host# set services jflow-log collector c1 destination-address 2.2.2.3
destination-port 1 source-ip 1.2.3.1
user@host# set services jflow-log collector-group cg1 collector c1
```

3. Configure the template profiles and associate the template profile with the collector or collector group.

```
[edit]
user@host# set services jflow-log template-profile template-profile-name collector
collector-name version (ipfix | v9) template-type nat refresh-rate packets packets
seconds seconds
user@host# set services jflow-log template-profile template-profile-name
collector-group collector-group-name version (ipfix | v9) template-type nat
refresh-rate packets packets seconds seconds
```

For example:

```
[edit]
user@host# set services jflow-log template-profile t1 collector c1 version ipfix
template-type nat refresh-rate packets 20 seconds 20
user@host# set services jflow-log template-profile t1 collector-group cg1
user@host# set services jflow-log template-profile t2 collector c2 version v9
template-type nat refresh-rate packets 20 seconds 20
```

4. Associate the template profile with the service set.

```
[edit]
user @ host# set services service-set service-set-name jflow-log template-profile
template-profile-name
```

For example:

```
[edit]
user @ host# set services service-set sset_0 jflow-log template-profile t1
```

Related Documentation

- [Logging NAT Events in Flow Monitoring Format Overview on page 48](#)
- [Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57](#)
- [Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69](#)

Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting

You can configure MX Series routers with MS-MPCs and MS-MICs to log network address translation (NAT) events using the Junos Traffic Vision (previously known as Jflow) version 9 or IPFIX (version 10) template format. This method of generating flow monitoring records for NAT events, such as NAT44 and NAT64 session creation and deletion, and NAT44 and NAT64 binding information base events, enables cohesive and streamlined analysis of NAT traffic and troubleshooting of NAT-related problems.



NOTE: This functionality is supported on MX Series routers with Junos OS Extension-Provider packages installed and configured on the device, and on MS-MPCs and MS-PICs. It is not supported on MS-DPCs with MX Series routers.

This example describes how to configure flow monitoring log generation in flow monitoring format for NAT events at the service-set level on MS-MIC and MS-MPC, and contains the following sections:

- [Requirements on page 70](#)
- [Generation of Log Messages Using Flow Templates for NAT Operations on MS-MPCs and MS-MCs on page 70](#)
- [Configuration on page 70](#)
- [Verification on page 73](#)

Requirements

This example uses the following hardware and software components:

- One MX Series router with an MS-MPC or MS-MIC.
- Junos OS Release 14.2R2 or later for MX Series routers

Generation of Log Messages Using Flow Templates for NAT Operations on MS-MPCs and MS-MCs

You can configure the mechanism to record logging messages in flow monitoring format for NAT events. You can create a template profile for a particular NAT service on an MX Series router with MS-MPCs or MS-MICs, or for a service set, which applies for all of the NAT services. You must define a template profile to generate flow monitoring logs in a specific flow template format and attach the template profile with a service set. You must configure a collector or a group of collectors, which are hosts that receive the log messages for NAT events from the service PIC or the exporter. You need to associate a template profile with the collector. The profile defines the characteristics of the flow monitoring record template, such as the version of flow monitoring (version 9 or IPFIX), the refresh rate, in either packets or seconds, and the type of service or application (NAT in this case) for which flow records must be sent to the collector.

Assume a sample deployment in which two collectors, c1 and c2, are defined. These collectors are clustered into two groups. The collector group, cg1, contains c1 and c2, and the collector group, cg2, contains c2. Two template profiles named t1 and t2 are defined. The profiles, t1 and t2, are associated with collectors, c1 and c2, respectively.

These profiles describe the properties or attributes for transmission of logs, such as the flow template format to be used, the rate at which the logs must be refreshed, and the service or event, such as NAT, for which logs must be sent to the specified collector.

Configuration

To enable the flow monitoring log capability for NAT events and configure the transmission of logs to collectors, perform these tasks:

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 Service Set Properties	<code>set services service-set sset_0 interface-service service-interface ms-5/0/0.0</code>
Applying Flow Monitoring Log Service on an Interface	<code>set interfaces ms-5/0/0 services-options jflow-log message-rate-limit 50000</code>
Enabling and Configuring Flow Monitoring Logs for a Service Set	<pre> set services jflow-log collector c1 destination-address 2.2.2.3 destination-port 1 source-ip 1.2.3.1 set services jflow-log collector c2 destination-address 5.5.5.5 destination-port 3 source-ip 1.2.3.2 set services jflow-log collector-group cg1 collector [c1 c2] set services jflow-log template-profile t1 collector c1 version ipfix template-type nat refresh-rate packets 20 seconds 20 set services jflow-log template-profile t2 collector c2 version v9 template-type nat refresh-rate packets 20 seconds 20 set services jflow-log template-profile t1 collector-group cg1 </pre>
Associating the Template Profile with a Service Set	<code>set services service-set sset_0 jflow-log template-profile t1</code>
Step-by-Step Procedure	<p>To configure the generation and transmission of flow monitoring template logs for NAT events:</p> <ol style="list-style-type: none"> 1. Create a service set properties. <pre> [edit] user@host# set services service-set sset_0 interface-service service-interface ms-5/0/0.0 </pre> 2. Define the flow monitoring log service to be applied on an interface. <pre> [edit] user@host# set interfaces ms-5/0/0 services-options jflow-log message-rate-limit 50000 </pre> 3. Configure the collectors and collector groups. <pre> [edit] user@host# set services jflow-log collector c1 destination-address 2.2.2.3 destination-port 1 source-ip 1.2.3.1 user@host# set services jflow-log collector c2 destination-address 5.5.5.5 destination-port 3 source-ip 1.2.3.2 user@host# set services jflow-log collector-group cg1 collector [c1 c2] user@host# set services jflow-log collector-group cg2 collector c2 </pre> 4. Configure the template profiles and associate the template profile with the collector. <pre> [edit] user@host# set services jflow-log template-profile t1 collector c1 version ipfix template-type nat refresh-rate packets 20 seconds 20 user@host# set services jflow-log template-profile t2 collector c2 version v9 template-type nat refresh-rate packets 20 seconds 20 </pre> 5. Associate the template profile with the service set. <pre> [edit] user @ host# set services service-set sset_0 jflow-log template-profile t1 </pre>

Results

From the configuration mode, confirm your configuration by entering the **show services**, **show services jflow-log**, and **show services service-set sset_0 jflow-log** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show services
service-set sset_0 {
    interface-service {
        service-interface ms-5/0/0;
    }
}

[edit interfaces]
ms-5/0/0 {
    services-options {
        jflow-log {
            message-rate-limit 50000;
        }
    }
}

user@host# show services jflow-log
collector c1 {
    destination-address 2.2.2.3;
    destination-port 1;
    source-ip 1.2.3.1;
}
collector c2 {
    destination-address 5.5.5.5;
    destination-port 3;
    source-ip 1.2.3.2;
}
collector-group cg1 {
    collector [ c2 c1 ];
}
collector-group cg2 {
    collector c2;
}
template-profile t2 {
    collector c2;
    template-type nat;
    refresh-rate packets 20 seconds 20;
    version v9;
}
template-profile t1 {
    collector c1;
    template-type nat;
    refresh-rate packets 20 seconds 20;
    version ipfix;
}

[edit]
user@host# show services service-set sset_0 jflow-log
template-profile t2;
```

Verification

To confirm that the configuration is working properly, perform the following:

- [Verifying That the Flow Monitoring Logs Are Generated and Sent to Collectors on page 73](#)

Verifying That the Flow Monitoring Logs Are Generated and Sent to Collectors

Purpose Verify that the flow monitoring log messages in the defined template format, such as IPFIX or version 9, are generated and transmitted to the configured collectors for the different NAT operations.

Action From operational mode, use the **show services service-sets statistics jflow-log** command:

```
user@host> show services service-sets statistics jflow-log
Interface: ms-5/0/0
  Rate limit: 1000
  Template records:
    Sent: 36
    Dropped: 0
  Data records:
    Sent: 2
    Dropped: 0

  Service-set: sset_0
    Unresolvable collectors: 0
    Template records:
      Sent: 36
      Dropped: 0
    Data records:
      Sent: 2
      Dropped: 0
```

From operational mode, use the **show services service-sets statistics jflow-log detail** command:

```
user@host> show services service-sets statistics jflow-log detail

Interface: ms-5/0/0
  Rate limit: 1000
  Template records:
    Sent: 48
    Dropped: 0
  Data records:
    Sent: 4
    Dropped: 0

  Service-set: sset_0
    Unresolvable collectors: 0
    Template records:
      Sent: 48
      Dropped: 0
    Data records:
      Sent: 4
      Dropped: 0
```

NAT44 Session logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 4
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 Session logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 BIB logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 BIB logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT Address Exhausted logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT Port Exhausted logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 Quota Exceeded logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 Quota Exceeded logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 Address Bind logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:

```
Sent: 0
Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 Address Bind logs:
Template records:
Sent: 4
Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
Sent: 0
Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 PBA logs:
Template records:
Sent: 4
Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
Sent: 0
Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 PBA logs:
Template records:
Sent: 4
Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
Sent: 0
Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
```

Meaning The output shows that the log messages in flow monitoring format associated with the specified service set and interface are generated for the different NAT events.

- Related Documentation**
- [Logging NAT Events in Flow Monitoring Format Overview on page 48](#)
 - [Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57](#)
 - [Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68](#)

PART 2

Flow Capture Services

- [Dynamically Capturing Packet Flows Using Junos Capture Vision on page 79](#)
- [Detecting Threats and Intercepting Flows Using Junos Packet Vision on page 91](#)

CHAPTER 5

Dynamically Capturing Packet Flows Using Junos Capture Vision

- [Understanding Junos Capture Vision on page 79](#)
- [Configuring Junos Capture Vision on page 81](#)
- [Example: Configuring Junos Capture Vision on page 87](#)

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 79](#)
- [Liberal Sequence Windowing on page 80](#)
- [Intercepting IPv6 Flows on page 81](#)

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.

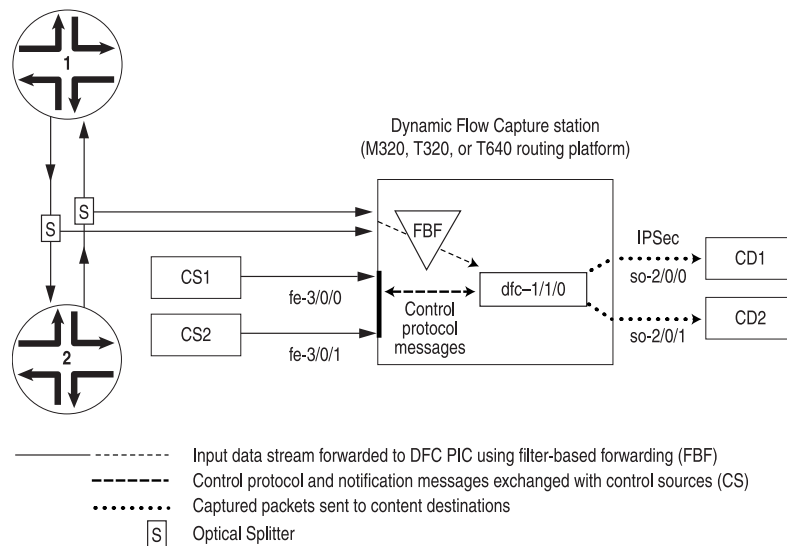
- Content destination—Recipient of the matched packets from the monitoring platform. Typically the matched packets are sent using an IP Security (IPsec) tunnel from the monitoring platform to another router connected to the content destination. The content destination and the control source can be physically 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 4 on page 80 shows a sample topology. The number of control sources and content destinations is arbitrary.

Figure 4: Junos Capture Vision Topology



g017075

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 81](#)
 - [Example: Configuring Junos Capture Vision on page 87](#)

Configuring Junos Capture Vision

This section describes the following tasks for configuring Junos Capture Vision:

- [Configuring the Capture Group on page 81](#)
- [Configuring the Content Destination on page 82](#)
- [Configuring the Control Source on page 83](#)
- [Configuring the DFC PIC Interface on page 84](#)
- [Configuring the Firewall Filter on page 85](#)
- [Configuring System Logging on page 85](#)
- [Configuring Tracing Options for Junos Capture Vision Events on page 86](#)
- [Configuring Thresholds on page 86](#)
- [Limiting the Number of Duplicates of a Packet on page 87](#)

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 79](#)
- [Example: Configuring Junos Capture Vision on page 87](#)

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 "$ABC123";
            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 26](#).

```
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 79](#)
 - [Configuring Junos Capture Vision on page 81](#)

CHAPTER 6

Detecting Threats and Intercepting Flows Using Junos Packet Vision

- [Understanding Junos Packet Vision on page 91](#)
- [Junos Packet Vision Architecture on page 92](#)
- [Configuring Junos Packet Vision on page 93](#)
- [Configuring FlowTapLite on page 96](#)
- [Examples: Configuring Flow-Tap Services on page 97](#)

Understanding Junos Packet Vision

Junos Capture Vision (previously known as dynamic flow capture) enables you to capture packet flows on the basis of dynamic filtering criteria, using Dynamic Tasking Control Protocol (DTCP) requests. Junos Packet Vision is a Junos OS application that performs lawful intercept of packet flows, using Dynamic Tasking Control Protocol (DTCP). The application extends the use of DTCP 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. Junos Packet Vision was previously known as flow-tap application.

Junos Packet Vision data can be used in the following applications:

- Flexible trend analysis for detection of new security threats
- Lawful intercept

Junos Packet Vision is supported on M Series and T Series routers, except M160 and TX Matrix routers. Junos Packet Vision filters are applied on all IPv4 traffic and do not add any perceptible delay in the forwarding path. Junos Packet Vision 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.

Related Documentation

- [Junos Packet Vision Architecture on page 92](#)
- [Configuring Junos Packet Vision on page 93](#)
- [Configuring FlowTapLite on page 96](#)
- [Examples: Configuring Junos Packet Vision on page 97](#)

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;
    }
  }
}
```

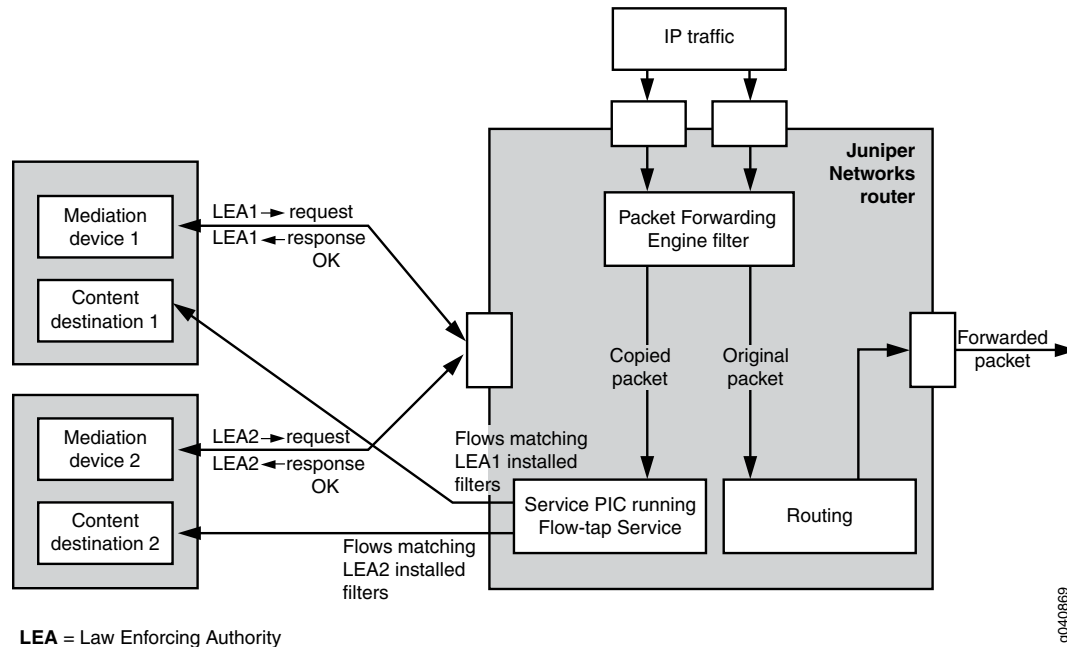
```

    then {
      flow-tap;
    }
  }
}

```

Figure 5 on page 93 shows a sample topology that uses two mediation devices and two content destinations.

Figure 5: Junos Packet Vision Topology



Related Documentation

- [Understanding Junos Packet Vision on page 91](#)
- [\[edit services flow-tap\] Hierarchy Level on page 335](#)
- [Configuring Junos Packet Vision on page 93](#)
- [Examples: Configuring Junos Packet Vision on page 97](#)

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 93](#)
- [Strengthening Junos Packet Vision Security on page 94](#)
- [Restrictions on Junos Packet Vision Services on page 95](#)

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 96](#)). 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 96](#)

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 on page 91](#)
- [\[edit services flow-tap\] Hierarchy Level on page 335](#)
- [Configuring Junos Packet Vision on page 93](#)
- [Examples: Configuring Junos Packet Vision on page 97](#)

Examples: Configuring Flow-Tap Services

The following example shows all parts of a complete flow-tap configuration. The example configuration intercepts IPv4 and IPv6 flows.

```

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:

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 "$ABC123"; ## 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 on page 91](#)
- [\[edit services flow-tap\] Hierarchy Level on page 335](#)
- [Configuring Junos Packet Vision on page 93](#)
- [Configuring FlowTapLite on page 96](#)

PART 3

Sampling, Discard Accounting, and Port Mirroring Services

- [Sampling Data Using Traffic Sampling and Discard Accounting on page 103](#)
- [Sampling Data Using Inline Sampling on page 117](#)
- [Sampling Data Using Flow Aggregation on page 131](#)
- [Sending Packets for Analysis Using Port Mirroring on page 173](#)

CHAPTER 7

Sampling Data Using Traffic Sampling and Discard Accounting

- [Configuring Traffic Sampling on page 103](#)
- [Sampling Instance Configuration on page 114](#)
- [Configuring Discard Accounting on page 115](#)

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 one of the following three 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.
- On an inline data path without the need for a services Dense Port Concentrator (DPC). To do this inline active sampling, 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. Inline sampling supports version 9 and IPFIX flow collection templates.



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 104](#)
- [Configuring Traffic Sampling on a Logical Interface on page 105](#)
- [Disabling Traffic Sampling on page 107](#)
- [Sampling Once on page 107](#)
- [Preserving Prerewrite ToS Value for Egress Sampled or Mirrored Packets on page 107](#)
- [Configuring Traffic Sampling Output on page 108](#)

- [Tracing Traffic Sampling Operations on page 110](#)
- [Traffic Sampling Examples on page 111](#)

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 Policies, Firewall Filters, and Traffic Policers 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.



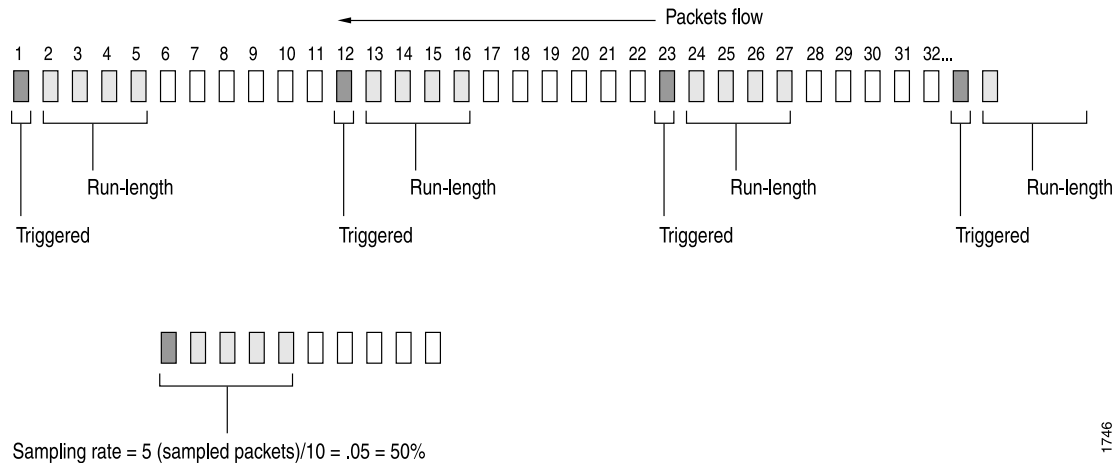
NOTE: When you configure active monitoring and specify a Monitoring Services, Adaptive Services, or Multiservices PIC in the output statement, the `max-packets-per-second` value is ignored.

Specify the sampling rate by setting the values for `rate` and `run-length` (see [Figure 6 on page 106](#)).

Figure 6: Configuring Sampling Rate

Rate and Run-length

Case #1 Rate =10, run-length =4



1746



NOTE: If PIC-based flow monitoring is enabled on an *ms-fpc/pic/port.logical-unit* interface, a commit check error occurs when you attempt to configure ingress traffic sampling on that interface. This error occurs because a combination of ingress sampling and PIC-based flow monitoring operations on an ms- logical interface causes undesired flow monitoring behavior and might result in repeated sampling of a single packet. You must not configure ingress sampling on ms- logical interfaces on which PIC-based flow monitoring is enabled.

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=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 Active flow Monitoring” on page 122](#).

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 132](#).

The **aggregate-export-interval** statement is described in [“Configuring Discard Accounting” on page 115](#), and the **flow-active-timeout** and **flow-inactive-timeout** statements are described in [“Configuring Flow Monitoring” on page 6](#).

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
                                len num frag flags
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 111](#)
- [Example: Sampling All Traffic from a Single IP Address on page 112](#)
- [Example: Sampling All FTP Traffic on page 113](#)

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 114](#)

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* 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 Flow Monitoring](#)
- [Configuring Active Flow Monitoring](#)
- [Directing Traffic Sampling Output to a Server Running the cflowd Application](#)
- [Configuring Traffic Sampling on page 103](#)
- [Example: Sampling Instance Configuration](#)
- [\[edit forwarding-options sampling\] Hierarchy Level](#)
- [Inline Flow Monitoring for Virtual Chassis Overview](#)

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 132](#). The **flow-active-timeout** and **flow-inactive-timeout** statements are described in [“Configuring Flow Monitoring” on page 6](#).

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 132](#)
 - [Configuring Flow Monitoring on page 6](#)

CHAPTER 8

Sampling Data Using Inline Sampling

- [Understanding Inline Active Flow Monitoring on page 117](#)
- [Configuring Inline Active Flow Monitoring on page 122](#)
- [Configuring Inline Active Flow Monitoring on MX80 Routers on page 125](#)
- [Monitoring Network Traffic Flow Using Inline Flow Monitoring on PTX Series Routers on page 127](#)

Understanding Inline Active Flow Monitoring

This topic provides an overview of the inline active flow monitoring feature and IPFIX and Version 9 flow collection templates used for inline active flow monitoring.

This topic contains the following sections:

- [Inline Active Flow Monitoring on page 117](#)
- [Inline Active Flow Monitoring Limitations and Restrictions on page 118](#)
- [IPFIX and Version 9 Templates on page 120](#)

Inline Active Flow Monitoring

The inline active flow monitoring is implemented on the Packet Forwarding Engine. All the functions like flow creation, flow update, and flow records export are done by the Packet Forwarding Engine. The flow records are sent out in industry standard IPFIX format.

Inline active flow monitoring provides for higher scalability and performance as the scaling and performance are not dependent on the capacity of the services interface. It is also cost effective in more than one way as there is no need to invest in additional hardware or to dedicate a PIC slot for the services PIC. You can make full use of the available slots for handling traffic on the device.

Junos OS Release 13.2 extends inline active flow monitoring support to VPLS flows. Now, you can configure inline active flow monitoring for IPv4, IPv6, and VPLS traffic.

The inline active flow monitoring configuration can be broadly classified into four categories:

1. Configurations at the **[edit services flow-monitoring]** hierarchy level—At this level, you configure the template properties for inline flow monitoring.
2. Configurations at the **[edit forwarding-options]** hierarchy level—At this level, you configure a sampling instance and associate the template (configured at the **[edit services flow-monitoring]** hierarchy level) with the sampling instance. At this level, you also configure the flow-server IP address and port number as well as the flow export rate.
3. Configurations at the **[edit chassis]** hierarchy level—At this level, you associate the sampling instance with the FPC on which the media interface is present. If you are configuring sampling of IPv6 flows, you must also specify the flow hash table size.
4. Configurations at the **[edit firewall]** hierarchy level—At this level you configure a firewall filter for the family of traffic to be sampled. You must attach this filter to the interface on which you want to sample the traffic.

Inline active flow monitoring 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.

Before you configure inline active flow monitoring, 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: Starting with Junos OS Release 13.3, you can configure flow collectors to be reachable through non-default VPN routing and forwarding (VRF) instances by including the `routing-instance instance-name` statement at the **[edit forwarding-options sampling instance instance-name family (inet | inet6 | mpls) output flow-server hostname]** hierarchy level for inline flow monitoring. You cannot configure a flow collector to be reachable through non-default VRF instances for version 5 and version 8 flows. You must configure the routing instance to be a VRF instance by including the `instance-type vrf` statement at the **[edit routing-instances instance-name]** hierarchy level.

Inline Active Flow Monitoring Limitations and Restrictions

The following limitations and restrictions apply to the inline active flow monitoring feature in Junos OS:

- You can configure inline active flow monitoring only on MX Series routers with Trio-based line cards and T4000 routers with Type 5 FPCs.
- You can apply Version 9 flow template only to IPv4 traffic.
- You can configure only one sampling instance on an Flexible PIC Concentrator (FPC).

- You can configure only one type of sampling—either PIC-based sampling or inline sampling—per family in a sampling instance. However, you can configure PIC-based and inline sampling for different families in a sampling instance.
- You can configure only one collector for inline active flow monitoring.
- 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.
 - 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.
- 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.
- 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 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.

IPFIX and Version 9 Templates

The following sections list the fields included in IPFIX and Version 9 templates.

Fields Included in the IPFIX IPv4 Template

- IPv4 Source Address
- IPv4 Destination Address
- IPv4 TOS
- IPv4 Protocol
- L4 Source Port
- L4 Destination Port
- ICMP Type and Code
- Input Interface
- VLAN ID
- IPv4 Source Mask
- IPv4 Destination Mask
- Source AS
- Destination AS
- IPv4 Next Hop Address
- TCP Flags
- Output Interface
- Number of Flow Bytes
- Number of Flow Packets
- Minimum TTL (time to live)
- Maximum TTL (time to live)
- Flow Start Time
- Flow End Time
- Flow End Reason
- 802.1Q VLAN identifier (dot1qVlanId)
- 802.1Q Customer VLAN identifier (dot1qCustomerVlanId)

Fields Included in the IPFIX IPv6 Template

- IPv6 Source Address
- IPv6 Destination Address
- IPv6 TOS
- IPv6 Protocol
- L4 Source Port
- L4 Destination Port
- ICMP Type and Code
- Input Interface
- VLAN ID
- IPv6 Source Mask
- IPv6 Destination Mask
- Source AS
- Destination AS
- IPv6 Next Hop Address
- TCP Flags
- Output Interface
- Number of Flow Bytes
- Number of Flow Packets
- Minimum Hop Limits
- Maximum Hop Limits
- Flow Start Time
- Flow End Time
- Flow End Reason
- 802.1Q VLAN identifier (dot1qVlanId)
- 802.1Q Customer VLAN identifier (dot1qCustomerVlanId)

Fields Included in the Version 9 IPv4 Template

- IPv4 Source Address
- IPv4 Destination Address
- IPv4 TOS
- IPv4 Protocol
- L4 Source Port

- L4 Destination Port
- ICMP Type and Code
- Input Interface
- VLAN ID
- IPv4 Source Mask
- IPv4 Destination Mask
- Source AS
- Destination AS
- IPv4 Next Hop Address
- BGP IPv4 Next Hop Address
- TCP Flags
- Output Interface
- Number of Flow Bytes
- Number of Flow Packets
- Time when the first packet of the flow was switched.
- Time when the last packet of flow was switched.
- Internet Protocol Version

**Related
Documentation**

- *Example: Configuring Inline Active Flow Monitoring*
- [Configuring Inline Active Flow Monitoring on MX80 Routers on page 125](#)

Configuring Inline Active Flow Monitoring

The inline active flow monitoring is implemented on the Packet Forwarding Engine. All the functions like flow creation, flow update, and flow records export are done by the Packet Forwarding Engine. The flow records are sent out in industry standard IPFIX format.

The inline active flow monitoring configuration can be broadly classified into four categories:

1. Configurations at the **[edit services flow-monitoring]** hierarchy level—At this level, you configure the template properties for inline flow monitoring.
2. Configurations at the **[edit forwarding-options]** hierarchy level—At this level, you configure a sampling instance and associate the template (configured at the **[edit services flow-monitoring]** hierarchy level) with the sampling instance. At this level, you also configure the flow-server IP address and port number as well as the flow export rate.
3. Configurations at the **[edit chassis]** hierarchy level—At this level, you associate the sampling instance with the FPC on which the media interface is present. If you are

configuring sampling of IPv6 flows, you must also specify the flow hash table size.

4. Configurations at the **[edit firewall]** hierarchy level—At this level you configure a firewall filter for the family of traffic to be sampled. You must attach this filter to the interface on which you want to sample the traffic.

Before you configure inline active flow monitoring, 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 1024. When anticipated traffic volume requires larger tables, allocate larger tables.



NOTE: The functionality to log the cflowd records in a log file before they are exported to a cflowd server (by including the `local-dump` statement at the `[edit forwarding-options sampling instance instance-name family (inet | inet6 | mpls) output flow-server hostname]` hierarchy level) is not supported when you configure inline flow monitoring (by including the `inline-jflow` statement at the `[edit forwarding-options sampling instance instance-name family inet output]` hierarchy level).

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.

To configure inline active flow monitoring on all other MX Series routers (except for MX80 routers), EX Series switches, and T4000 routers with Type 5 FPC:

1. Enable inline active flow monitoring 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” on page 147](#).

The following is an example of the sampling configuration for an instance that supports inline active flow monitoring 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: On routers with Multiservices PICs or Multiservices DPCs, IPv4 and IPv6 fragments are processed accurately. The flow monitoring application creates two flows for every fragmented flow. The first fragment that has the complete Layer 4 information forms the first flow with 5-tuple data and subsequently, all the fragmented packets related to this flow form another flow with the Layer 4 fields set to zero.

**Related
Documentation**

- [Configuring Inline Active Flow Monitoring on MX80 Routers on page 125](#)
- [inline-jflow on page 410](#)

Configuring Inline Active Flow Monitoring on MX80 Routers

To configure inline active flow monitoring 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” on page 147](#).

The following is an example of the sampling configuration for an instance that supports inline active flow monitoring 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 on page 147](#)
- [Configuring Inline Active flow Monitoring on page 122](#)
- [inline-jflow on page 410](#)

Monitoring Network Traffic Flow Using Inline Flow Monitoring on PTX Series Routers

This topic describes how to configure inline flow monitoring so that you can use it to monitor your network traffic flow. This procedure applies to PTX Series routers that have third-generation FPCs installed.

Inline flow monitoring is implemented on the Logical CPU (LCPU). All the functions like flow creation, flow update, and flow records export are done by the LCPU. The flow records are sent out in the industry standard IPFIX format.

The inline flow monitoring configuration can be broadly classified into the following categories:

- Configurations at the **[edit services flow-monitoring version-ipfix template]** hierarchy level—At this level, you configure the template properties for inline flow monitoring.
- Configurations at the **[edit forwarding-options sampling instance]** hierarchy level—At this level, you configure a sampling instance and associate the template to the sampling instance. At this level, you also configure the flow-server IP address and port number as well as the autonomous system type.

- Configurations at the **[edit chassis fpc]** hierarchy level—At this level, you associate the sampling instance with the FPC on which the media interface is present.
- Configurations at the **[edit firewall]** hierarchy level—At this level you configure a firewall filter for the family of traffic to be sampled. You must attach this filter to the interface on which you want to sample the traffic.

To configure inline flow monitoring on PTX Series routers:

1. Enable inline flow monitoring and specify the source address.

```
[edit forwarding-options sampling instance instance-name family inet output
flow-server]
user@host# set inline-jflow source address source ip address
```

2. Specify the IPFIX output format.

```
[edit forwarding-options sampling instance instance-name family inet output flow-server
ip address]
user@host# set version-ipfix template ipv4-template
```

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 on PTX Series Routers” on page 152](#).

The following is an example of the sampling configuration for an instance that supports inline flow monitoring on **family inet** and 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;
                }
            }
        }
    }
}

```

- Related Documentation**
- [version-ipfix on page 532](#)
 - [Configuring Flow Aggregation to Use IPFIX Flow Templates on PTX Series Routers on page 152](#)

CHAPTER 9

Sampling Data Using Flow Aggregation

- Understanding Flow Aggregation on page 131
- Enabling Flow Aggregation on page 132
- Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd on page 132
- Configuring Flow Aggregation to Use Version 9 Flow Templates on page 137
- Configuring Flow Aggregation to Use IPFIX Flow Templates on page 147
- Configuring Flow Aggregation to Use IPFIX Flow Templates on PTX Series Routers on page 152
- Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows on page 157
- Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 160
- Inclusion of Fragmentation Identifier and IPv6 Extension Header Elements in IPFIX Templates on page 165
- Directing Replicated Flows to Multiple Flow Servers on page 167
- Logging cflowd Flows Before Export on page 170

Understanding Flow Aggregation

You can collect an aggregate of sampled flows and send the aggregate to a specified host that runs either the cflowd application available from CAIDA (<http://www.caida.org>) or the newer version 9 format defined in RFC 3954, *Cisco Systems NetFlow Services Export Version 9*. Before you can perform flow aggregation, the routing protocol process must export the autonomous system (AS) path and routing information to the sampling process.

By using flow aggregation, you can obtain various types of byte and packet counts of flows through a router. The application collects the sampled flows over a period of 1 minute. At the end of the minute, the number of samples to be exported are divided over the period of another minute and are exported over the course of the same minute.

You configure flow aggregation in different ways, depending on whether you want to export flow records in cflowd version 5 or 8 format, or the separate version 9 format. The latter allows you to sample MPLS, IPv4, IPv6, and peer AS billing traffic. You can also combine configuration statements between the MPLS and IPv4 formats.



NOTE: When PIC-based sampling is enabled, collection of flow statistics for sampled packets on flows in virtual private networks (VPNs) is also supported. No additional CLI configuration is required.

**Related
Documentation**

- [Enabling Flow Aggregation on page 132](#)
- [Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd on page 132](#)
- [Configuring Flow Aggregation to Use Version 9 Flow Templates on page 137](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 167](#)
- [Logging cflowd Flows Before Export on page 170](#)

Enabling Flow Aggregation

Before you can perform flow aggregation, the routing protocol process must export the autonomous system (AS) path and routing information to the sampling process. To enable the export of AS path and the routing information to the sampling process, one or more of the following needs to be configured:

- 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 on page 131](#)
- [Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd on page 132](#)
- [Configuring Flow Aggregation to Use Version 9 Flow Templates on page 137](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 167](#)
- [Configuring Traffic Sampling on page 103](#)
- [Logging cflowd Flows Before Export on page 170](#)

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.example.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 173](#).

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 Routing Engine- 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 Routing Engine- 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 Routing Engine- 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 Routing Engine-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 on page 131](#)
- [Enabling Flow Aggregation on page 132](#)
- [Configuring Flow Aggregation to Use Version 9 Flow Templates on page 137](#)
- [Configuring Flow Aggregation to Use IPFIX Flow Templates on page 147](#)

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* 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 137](#)
- [Configuring the Version 9 Template Properties on page 138](#)
- [Customizing Template ID, Observation Domain ID, and Source ID for Version 9 flow Templates on page 139](#)
- [Restrictions on page 140](#)
- [Fields Included in Each Template Type on page 141](#)
- [MPLS Sampling Behavior on page 142](#)
- [Verification on page 143](#)
- [Examples: Configuring Version 9 Flow Templates on page 143](#)

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), 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 157](#) and [“Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows” on page 160](#).

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
- Source autonomous system (AS) number
- Destination AS number

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 *MPLS Applications Feature Guide 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 ingressing 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 on page 131](#)
- [Enabling Flow Aggregation on page 132](#)
- [Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd on page 132](#)
- [Configuring Flow Aggregation to Use IPFIX Flow Templates on page 147](#)
- [Configuring Traffic Sampling on page 103](#)

Configuring Flow Aggregation to Use IPFIX Flow Templates

Use of IPFIX allows you to define a flow record template suitable for IPv4 traffic or IPv6 traffic. Templates are transmitted to the collector periodically, and the collector does not have to be aware of the router configuration. You can define template refresh rate, flow active timeout and inactive timeout.

If flow records are being sent for multiple protocol families (for example, for IPv4 and IPv6), each protocol family flow will have a unique Observation Domain ID.

The following sections contain additional information:

- [Configuring the IPFIX Template Properties on page 147](#)
- [Restrictions on page 148](#)
- [Customizing Template ID, Observation Domain ID, and Source ID for IPFIX flow Templates on page 148](#)
- [Fields Included in the IPv4 Template on page 149](#)
- [Fields Included in the IPv6 Template on page 150](#)
- [Verification on page 151](#)
- [Example: Configuring an IPFIX Flow Templates and Flow Sampling on page 151](#)

Configuring the IPFIX Template Properties

To define the IPFIX templates, include the following statements at the **[edit services flow-monitoring version-ipfix]** hierarchy level:

```
[edit services flow-monitoring IPFIX]
template name {
  options-template-id
  template-id
  observation-domain-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);
}
```

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** or **ipv6-template**.
- 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.

- 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 600 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;
      }
    }
  }
}

```

Restrictions

The following restrictions apply to IPFIX templates:

- 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 only after the route record resynchronization operation is complete, which takes 120 seconds.
- VLAN ID field is not valid for egress traffic, and returns a value of 0 for egress traffic.
- The VLAN ID field is updated when a new flow record is created and so, any change in VLAN ID after the record has been created might not be updated in the record.

Customizing Template ID, Observation Domain ID, and Source ID for IPFIX 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 version 9 templates for the different protocols or address families, until Junos OS Release 13.3:

- IPv4 flow template ID—272
- IPv6 flow template ID—273
- VPLS flow template ID—274
- Options template ID for all address families—520

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 157](#) and [“Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows” on page 160](#).

Fields Included in the IPv4 Template

- IPv4 Source Address
- IPv4 Destination Address
- IPv4 TOS
- IPv4 Protocol
- L4 Source Port
- L4 Destination Port
- ICMP Type and Code
- Input Interface
- VLAN ID
- IPv4 Source Mask
- IPv4 Destination Mask
- Source AS
- Destination AS
- IPv4 Next Hop Address
- TCP Flags
- Output Interface
- Number of Flow Bytes
- Number of Flow Packets

- Minimum TTL (time to live)
- Maximum TTL (time to live)
- Flow Start Time
- Flow End Time
- Flow End Reason
- 802.1Q VLAN identifier (dot1qVlanId)
- 802.1Q Customer VLAN identifier (dot1qCustomerVlanId)

Fields Included in the IPv6 Template

- IPv6 Source Address
- IPv6 Destination Address
- IPv6 TOS
- IPv6 Protocol
- L4 Source Port
- L4 Destination Port
- ICMP Type and Code
- Input Interface
- VLAN ID
- IPv6 Source Mask
- IPv6 Destination Mask
- Source AS
- Destination AS
- IPv6 Next Hop Address
- TCP Flags
- Output Interface
- Number of Flow Bytes
- Number of Flow Packets
- Minimum Hop Limits
- Maximum Hop Limits
- Flow Start Time
- Flow End Time
- Flow End Reason
- 802.1Q VLAN identifier (dot1qVlanId)
- 802.1Q Customer VLAN identifier (dot1qCustomerVlanId)

- Fragment Identification
- IPv6 Extension Headers

Verification

The following show commands are supported for IPFIX:

- **show services accounting flow inline-jflow fpc-slot *fpc-slot***
- **show services accounting errors inline-jflow fpc-slot *fpc-slot***
- **show services accounting status inline-jflow fpc-slot *fpc-slot***

Example: Configuring an IPFIX Flow Templates and Flow Sampling

The following is a sample IPFIX template configuration:

```
services {
  flow-monitoring {
    version-ipfix {
      template ipv4 {
        flow-active-timeout 60;
        flow-inactive-timeout 70;
        template-refresh-rate seconds 30;
        option-refresh-rate seconds 30;
        ipv4-template;
      }
    }
  }
}

chassis;
fpc 0 {
  sampling-instance s1;
}
```

The following example applies the IPFIX template to enable sampling of traffic for billing:

```
forwarding-options {
  sampling {
    instance {
      s1 {
        input {
          rate 10;
        }
        family inet {
          output {
            flow-server 11.11.4.2 {
              port 2055;
              version-ipfix {
                template {
                  ipv4;
                }
              }
            }
          }
        }
      }
    }
    inline-jflow {
```

```
        source-address 11.11.2.1;
    }
}
}
}
}
```

Related Documentation

- [Understanding Flow Aggregation on page 131](#)
- [Inclusion of Fragmentation Identifier and IPv6 Extension Header Elements in IPFIX Templates on page 165](#)
- [Enabling Flow Aggregation on page 132](#)
- [Configuring Flow Aggregation to Use Version 5 or Version 8 cflowd on page 132](#)
- [Configuring Flow Aggregation to Use Version 9 Flow Templates on page 137](#)

Configuring Flow Aggregation to Use IPFIX Flow Templates on PTX Series Routers

Use of IPFIX allows you to define a flow record template suitable for IPv4 traffic or IPv6 traffic. Templates are transmitted to the collector periodically, and the collector does not to be aware of the router configuration. You can define template refresh rate, flow active timeout and inactive timeout.

If flow records are being sent for multiple protocol families (for example, for IPv4 and IPv6), each protocol family flow will have a unique Observation Domain ID.

The following sections contain additional information:

- [Configuring the IPFIX Template Properties on page 152](#)
- [Restrictions on page 153](#)
- [Customizing Template ID, Observation Domain ID, and Source ID for IPFIX flow Templates on page 153](#)
- [Fields Included in the IPv4 Templates for PTX Series Routers on page 154](#)
- [Fields Included in the IPv6 Templates for PTX Series Routers on page 155](#)
- [Verification on page 156](#)
- [Example: Configuring an IPFIX Flow Templates and Flow Sampling on page 156](#)

Configuring the IPFIX Template Properties

To define the IPFIX templates, include the following statements at the **[edit services flow-monitoring version-ipfix]** hierarchy level:

```
[edit services flow-monitoring IPFIX]
template name {
  options-template-id
  template-id
  observation-domain-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);
}

```

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** or **ipv6-template**.
- 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.
- 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 600 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;
      }
    }
  }
}

```

Restrictions

The following restrictions apply to IPFIX templates:

- 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 only after the route record resynchronization operation is complete, which takes 120 seconds.

Customizing Template ID, Observation Domain ID, and Source ID for IPFIX flow Templates



NOTE: For PTX Series routers with third generation FPCs installed, the FPC's slot number is used for the observation domain ID.

Use of IPFIX flow templates allow 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 does not need to be aware of the router configuration. 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.

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.

Fields Included in the IPv4 Templates for PTX Series Routers

Table 19 on page 154 shows the fields that are available in the IPv4 templates.

Table 19: IPv4 Template Fields

Field	Element ID
IPv4 Source Address	8
IPv4 Destination Address	12
IPv4 TOS	5
IPv4 Protocol	4
L4 Source Port	7
L4 Destination Port	11
ICMP Type and Code	32
Input Interface	10
Source AS	16
Destination AS	17
BGP Next Hop Address	18
Output Interface	14
Number of Flow Bytes	1
Number of Flow Packets	2
Time the flow started with respect to system up time (FPC up time)	22

Table 19: IPv4 Template Fields (*continued*)

Field	Element ID
Time the flow ended with respect to system up time (FPC up time)	21
IPv4 Next Hop Address	15
IPv4 Source Mask	9
IPv4 Destination Mask	13
TCP Flags	6
IP Protocol Version	60
Time the flow started with respect to Epoch time	152
Time the flow ended with respect to Epoch time	153

Fields Included in the IPv6 Templates for PTX Series Routers

Table 19 on page 154 shows the fields that are available in the IPv6 templates.

Table 20: IPv6 Template Fields

Field	Element ID
IPv6 Source Address	27
IPv6 Destination Address	28
IPv6 TOS	5
IPv6 Protocol	4
L4 Source Port	7
L4 Destination Port	11
ICMP Type and Code	32
Input Interface	10
Source AS	16
Destination AS	17
Output Interface	14
Number of Flow Bytes	1

Table 20: IPv6 Template Fields (*continued*)

Field	Element ID
Number of Flow Packets	2
Time the flow started with respect to system up time (FPC up time)	22
Time the flow ended with respect to system up time (FPC up time)	21
IPv6 Next Hop Address	62
IPv6 Source Mask	29
IPv6 Destination Mask	30
TCP Flags	6
IP Protocol Version	60
Time the flow started with respect to Epoch time	152
Time the flow ended with respect to Epoch time	153

Verification

The following show commands are supported for IPFIX:

- **show services accounting flow inline-jflow fpc-slot *fpc-slot***
- **show services accounting errors inline-jflow fpc-slot *fpc-slot***
- **show services accounting status inline-jflow fpc-slot *fpc-slot***

Example: Configuring an IPFIX Flow Templates and Flow Sampling

The following is a sample IPFIX template configuration:

```

services {
  flow-monitoring {
    version-ipfix {
      template ipv4 {
        flow-active-timeout 60;
        flow-inactive-timeout 70;
        template-refresh-rate seconds 30;
        option-refresh-rate seconds 30;
        ipv4-template;
      }
    }
  }
}

chassis;
  fpc 0 {

```

```
sampling-instance s1;
}
```

The following example applies the IPFIX template to enable sampling of traffic for billing:

```
forwarding-options {
  sampling {
    instance {
      s1 {
        input {
          rate 10;
        }
        family inet {
          output {
            flow-server 11.11.4.2 {
              port 2055;
              version-ipfix {
                template {
                  ipv4;
                }
              }
            }
          }
          inline-jflow {
            source-address 11.11.2.1;
          }
        }
      }
    }
  }
}
```

Related Documentation

- [Configuring Inline Flow Monitoring on PTX Series Routers on page 127](#)
- [version-ipfix on page 532](#)
- [ipv4-template on page 419](#)
- [ipv6-template on page 421](#)

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 21 on page 159](#) 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 21: Example of Observation Domain ID

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
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 21: 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
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 160](#)

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 22 on page 162](#) describes the values of data template and option template IDs for different protocols with default and configured values for IPFIX flows.

Table 22: 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
VPLS	1024-65535	1024-65535	1024-65535
MPLS	None	259	579
MPLS	1024-65535	1024-65535	1024-65535

[Table 23 on page 162](#) describes the values of data template and option template IDs for different protocols with default and configured values for version 0 flows.

Table 23: Values of Template and Option Template IDs for Version 9 Flows

Family	Configured Value	Data Template	Option Template
IPv4	None	320	576

Table 23: Values of Template and Option Template IDs for Version 9 Flows (*continued*)

Family	Configured Value	Data Template	Option Template
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 24 on page 163 describes the values of data template and option template IDs for different protocols with default and configured values for IPFIX flows.

Table 24: 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

Table 24: 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
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
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

Table 24: 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
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 157](#)

Inclusion of Fragmentation Identifier and IPv6 Extension Header Elements in IPFIX Templates

Starting with Junos OS Release 14.2, the following attributes can be contained in IPFIX flow templates that are sent to the flow collector:

- fragmentIdentification (element ID 54)
- ipv6ExtensionHeaders (element ID 64)

A flow can receive many fragments in a given interval. For a given set of fragments of a packet, there is a unique fragment Identification. Hence, multiple such values can be received in a given interval. RFC 5102 for fragmentIdentification 54 does not clearly indicate which fragment identification needs to be shipped in the flow record information (first fragment observed after sending the flow record information or the last observed before shipping the flow record information). However, the last observed fragment Identification for a given flow is also transmitted to the flow collector.

Unlike in IPv4, IPv6 routers never fragment IPv6 packets. Packets exceeding the size of the maximum transmission unit of the destination link are dropped and this condition is signaled by a Packet Too Big ICMPv6 type 2 message to the originating node, similarly to the IPv4 method when the Don't Fragment (DF) bit is set.

The fragmentIdentification element is supported for both IPv4 and IPv6 flow templates. The fragmentIdentification element is added in the record template. The fragmentIdentification attribute is 32 bits in size for both IPv4 and IPv6. For IPv6, this field is present in fragment Extension header and Fragment Identifier is updated as 0 if there is no Fragment extension header.

Ports are a part of the key used to identify a Flow and the subsequent packets after the first fragmented packet does not have the port information. For a fragmented packet that is destined to the router, the packets that are split assume different flows (the first and the subsequent packets). Also, because the port is denoted as zeroes for fragmented packets, all the traffic destined to a particular destination from a particular source might be reported as the same flow, although no association exists between them in terms of destination ports. Fragment ID is not part of the key. Although the fragment ID attribute is unique between each source and destination, they might end up as same flows in the intermediate router.

With ports being used in the key for the flow lookup, the fragmented packets of a stream are accounted in two different flows. The first fragmented packet, which contains the port information in its packet, is part of one flow. Subsequent packets after the first fragments, which do not contain the port information, are accounted under a different flow. Because the second flow does not contain the port information to identify itself, it consolidates all the other traffic streams with same source IP and destination IP address prefixes (also includes the non-first fragmented packets sent on different ports).

Destination nodes or endpoints in IPv6 are expected to perform path MTU discovery to determine the maximum size of packets to send, and the upper-layer protocol is expected to limit the payload size. However, if the upper-layer protocol is unable to do so, the sending host may use the Fragment extension header in order to perform end-to-end fragmentation of IPv6 packets. Any data link layer conveying IPv6 data must be capable of delivering an IP packet containing 1280 bytes without the need to invoke end-to-end fragmentation at the IP layer.

The `ipv6ExtensionHeaders` information element is a set for 32 bit fields. Each bit in this set represents one IPv6 Extension header. An extension header bit is set if that particular extension header is observed for the flow. The bit is set to 1 if any observed packet of this Flow contains the corresponding IPv6 extension header. Otherwise, if no observed packet of this Flow contained the respective IPv6 extension header, the value of the corresponding bit is 0. The `ipv6ExtensionHeaders` element is added in the record template. The number of flows that are created depends on the number of IPv6 packets that include the IPv6 extender header attribute.

To enable the inclusion of element ID, 54, `fragmentIdentification` and element ID, 64, `ipv6ExtensionHeaders` in IPFIX flow templates that are exported to the flow collector, include the **`ipv6-extended-attrib`** statement at the **[`edit chassis fpc slot-number inline-services flow-table-size`]** hierarchy level. Collection of IP4 fragmentation IDs occurs automatically without having to configure this setting explicitly.

```
[edit chassis]
fpc slot-number {
  inline-services {
    flow-table-size {
      ipv6-extended-attrib;
    }
  }
}
```

[Table 25 on page 167](#) describes the values of the IPv6 options and their functions that are contained in IPv6 packets.

Table 25: Values of IPv6 Options and Extension Headers in Packets

Bit Value	IPv6 Option	Next Header Code	Description
0	Res	Not applicable	Reserved
1	FRA1	44	Fragmentation Header
2	RH	43	Routing Header
3	FRA0	44	Fragment Header – First Fragment
4	UNK	Not applicable	Unknown Layer 4 header (compressed, encrypted, not supported)
5	Res	Not applicable	Reserved
6	HOP	0	Hop-by-hop option header
7	DST	60	Destination option header
8	PAY	108	Payload compression header
9	AH	51	Authentication header
10	ESP	50	Encrypted security payload
11 through 31	Res	Not applicable	Reserved

Related Documentation

- [Configuring Flow Aggregation to Use IPFIX Flow Templates on page 147](#)
- [ipv6-extended-attrib on page 420](#)

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 168](#)
- [Directing Replicated Version 9 Flow Aggregates to Multiple Servers on page 168](#)

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 3](#)
- [Configuring Flow Monitoring on page 6](#)
- [Configuring Services Interface Redundancy with Flow Monitoring on page 21](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 11](#)

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 108](#).



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 3](#)
- [Configuring Flow Monitoring on page 6](#)
- [Directing Replicated Flows to Multiple Flow Servers on page 167](#)

- [Configuring Services Interface Redundancy with Flow Monitoring on page 21](#)
- [Example: Configuring Active Monitoring on Logical Systems on page 11](#)

CHAPTER 10

Sending Packets for Analysis Using Port Mirroring

- [Understanding Port Mirroring on page 173](#)
- [Configuring Port Mirroring on page 173](#)
- [Defining a Next-Hop Group for Port Mirroring on page 190](#)
- [Example: Multiple Port Mirroring with Next-Hop Groups Configuration on page 191](#)

Understanding Port Mirroring

On routers containing an Internet Processor II application-specific integrated circuit (ASIC) or T Series Internet Processor, you can send a copy of an IP version 4 (IPv4) or IP version 6 (IPv6) packet from the router to an external host address or a packet analyzer for analysis. This is known as *port mirroring*.

Port mirroring is different from traffic sampling. In traffic sampling, a sampling key based on the IPv4 header is sent to the Routing Engine. There, the key can be placed in a file, or cflowd packets based on the key can be sent to a cflowd server. In port mirroring, the entire packet is copied and sent out through a next-hop interface.

You can configure simultaneous use of sampling and port mirroring, and set an independent sampling rate and run-length for port-mirrored packets. However, if a packet is selected for both sampling and port mirroring, only one action can be performed and port mirroring takes precedence. For example, if you configure an interface to sample every packet input to the interface and a filter also selects the packet to be port mirrored to another interface, only the port mirroring would take effect. All other packets not matching the explicit filter port-mirroring criteria continue to be sampled when forwarded to their final destination.

Related Documentation

- [Configuring Port Mirroring on page 173](#)
- [Example: Multiple Port Mirroring with Next-Hop Groups Configuration on page 191](#)

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 family inet]
input {
  maximum-packet-length bytes;
  rate rate;
  run-length number;
}
family (inet|inet6) {
  output {
    interface interface-name {
      next-hop address;
    }
    no-filter-check;
  }
}
```

or

```
[edit forwarding-options port-mirroring]
input {
  maximum-packet-length bytes;
  rate rate;
  run-length number;
}
family inet6 {
  output {
    next-hop-group group-name{
      group-type inet6;
      interface interface-name {
        next-hop ipv6-address;
      }
    }
    next-hop-subgroup group-name{
      interface interface-name {
        next-hop ipv6-address;
      }
    }
  }
}
```




NOTE: The input statement can also be configured at the `[edit forwarding-options port-mirroring]` hierarchy level. This is only maintained for backward compatibility. However, the configuration of the output statement is deprecated 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.

You can also specify the port-mirroring destination by including the **next-hop-group** statement at the `[edit forwarding-options port-mirroring family inet6 output]` hierarchy level:

```
next-hop-group group-name {
  group-type inet6;
  interface interface-name {
    next-hop ipv6-address;
  }
  next-hop-subgroup group-name {
    interface interface-name {
      next-hop ipv6-address;
    }
  }
}
```

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 110](#).

For more information about port mirroring, see the following sections:

- [Configuring Tunnels on page 176](#)
- [Port Mirroring with Next-Hop Groups on page 178](#)

- [Configuring Inline Port Mirroring on page 179](#)
- [Filter-Based Forwarding with Multiple Monitoring Interfaces on page 180](#)
- [Restrictions on page 180](#)
- [Configuring Port Mirroring on Services Interfaces on page 181](#)
- [Examples: Configuring Port Mirroring on page 182](#)

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*.

The MX Series routers support Dense Port Concentrators (DPCs) with built-in Ethernet ports, which do not support Tunnel Services PICs. To create tunnel interfaces on an MX Series router with a DPC, you configure the DPC and the corresponding Packet Forwarding Engine to use for tunneling services at the **[edit chassis]** hierarchy level. You also configure the amount of bandwidth reserved for tunnel services. The Junos OS creates tunnel interfaces on the Packet Forwarding Engine.

To create tunnel interfaces on MX Series routers, include the following statements at the **[edit chassis]** hierarchy level:

```
[edit chassis]
fpc slot-number {
  pic number {
    tunnel-services {
      bandwidth bandwidth-value;
    }
  }
}
```

Include the **fpc slot-number** statement to specify the slot number of the DPC. If two SCBs are installed, the range is 0 through . If three SCBs are installed, the range is 0 through 5 and 7 through .

Include the **pic number** statement to specify the number of the Packet Forwarding Engine on the DPC. The range is 0 through 3.

You can also specify the amount of bandwidth to allocate for tunnel traffic on each Packet Forwarding Engine by including the **bandwidth bandwidth-value** statement at the **[edit chassis fpc slot-number pic pic-number]** hierarchy level:

- **1g** indicates that 1 Gbps of bandwidth is reserved for tunnel traffic. Configure this option only for a Packet Forwarding Engine on a Gigabit Ethernet 40-port DPC.
- **10g** indicates that 10 Gbps of bandwidth is reserved for tunnel traffic. Configure this option only for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC.
- **20g** or **40g**—Configure 20 gigabits per second or 40 gigabits per second only on an MX Series router with the MPC3E and the 100-Gigabit CFP MIC.

If you specify a bandwidth that is not compatible with the type of DPC and Packet Forwarding Engine, 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.

When you configure tunnel interfaces on the Packet Forwarding Engine of a 10-Gigabit Ethernet 4-port DPC, the Ethernet interfaces for that port are removed from service and are no longer visible in the command-line interface (CLI). The Packet Forwarding Engine of a 10-Gigabit Ethernet 4-port DPC supports either tunnel interfaces or Ethernet interfaces, but not both. Each port on the 10-Gigabit Ethernet 4-port DPC includes two LEDs, one for tunnel services and one for Ethernet services, to indicate which type of service is being used. On the Gigabit Ethernet 40-port DPC, you can configure both tunnel and Ethernet interfaces at the same time.

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.

For IPv6 port mirroring to reach next-hop destination, you can configure a **next-hop-group** statement at the **[edit forwarding-options port-mirroring family inet6 output]** hierarchy level:

```
next-hop-group group-name {
  group-type inet6;
  interface interface-name {
    next-hop ipv6-address;
  }
  next-hop-subgroup group-name {
    interface interface-name {
      next-hop ipv6-address;
    }
  }
}
```

Next-hop groups have the following restrictions:

- 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 or next-hop subgroups 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.
- Each next-hop subgroup supports up to 16 next-hop groups.

Port Mirroring with Next-Hop Groups

You can configure next-hop groups for M Series, MX Series, and TX Series routers using either IP addresses or Layer 2 addresses for the next hops. Use the **group-type [inet | inet6 | layer-2]** statement at **[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]** hierarchy level 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 MX Series routers with MPCs, 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 M Series, MX Series, 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 | inet6] 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 {
        interface interface-name {
          next-hop address;
        }
      }
    }
  }
}
or
[edit forwarding-options]
port-mirror {
  family inet6 {
    output {
      next-hop-group group-name {
        group-type inet6;
        interface interface-name {
          next-hop ipv6-address;
        }
      }
      next-hop-subgroup group-name {
        interface interface-name {
          next-hop ipv6-address;
        }
      }
    }
  }
}
```

```

    }
  }
}
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 182](#). This configuration is supported with IPv4 and IPv6 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 MX Series routers with 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 182](#).

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.
- Port mirroring in the ingress and egress direction is not supported for link services IQ (lsq-) interfaces.
- 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.
- 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 MX Series routers with 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-hop 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 inet6 {
  output {
    next-hop-group inet6_nhg6 {
      group-type inet6;
      interface ge-2/0/3.102 {
        next-hop 10::1:1:10;
      }
      interface ge-2/0/4.103 {
        next-hop 20::1:1:10;
      }
      next-hop-subgroup vpls_subg {
        interface ge-2/0/.101 {
          next-hop 3::1:1:1;
        }
        interface ge-2/2/9.1 {
          next-hop 4::1:1:1;
        }
      }
    }
  }
}
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 inet6 {
      output {
        next-hop-group inet6_nhg6;
      }
    }
    family vpls {
      output {
        next-hop-group vpls_nhg_2;
      }
    }
  }
}
}

```

The following example shows configuration of port mirroring using next-hop 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, PM2, and PM3 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;
        }
      }
    }
  }
  pm3 {
    input {
      rate 3;
    }
    family inet6 {
      output {
        interface ge-1/2/3.0 {
          next-hop 5::5:5:1;
        }
      }
    }
  }
}
firewall {
  filter pm_filter {
    term t1 {
      then port-mirror-instance pm2;
    }
  }
  filter nhg6_filter6 {
    term t6 {
      then next-hop-group inet6-nhg6;
    }
  }
}
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 on page 173](#)
- [Example: Multiple Port Mirroring with Next-Hop Groups Configuration on page 191](#)

Defining a Next-Hop Group for Port Mirroring

On routers containing an Internet Processor II application-specific integrated circuit (ASIC) or T Series Internet Processor, you can send a copy of an IP version 4 (IPv4) or IP version 6 (IPv6) packet from the router to an external host address or a packet analyzer for analysis. This is known as *port mirroring*.

Port mirroring is different from traffic sampling. In traffic sampling, a sampling key based on the IPv4 header is sent to the Routing Engine. There, the key can be placed in a file, or cflowd packets based on the key can be sent to a cflowd server. In port mirroring, the entire packet is copied and sent out through a next-hop interface.

You can configure simultaneous use of sampling and port mirroring, and set an independent sampling rate and run-length for port-mirrored packets. However, if a packet is selected for both sampling and port mirroring, only one action can be performed, and port mirroring takes precedence. For example, if you configure an interface to sample every packet input to the interface and a filter also selects the packet to be port mirrored to another interface, only the port mirroring would take effect. All other packets not matching the explicit filter port-mirroring criteria continue to be sampled when forwarded to their final destination.

Next-hop groups allow you to include port mirroring multiple interfaces used to forward duplicate packets used in port mirroring.

On MX Series routers, you can mirror tunnel interface input traffic to multiple destinations. To this form of multipacket port mirroring, you specify two or more additional destinations in a next-hop group, define a firewall filter that references the next-hop group as the filter action, and then apply the filter to a logical tunnel interface (lt-) or virtual tunnel interface (vt-) on the MX Series router.

To define a next-hop group for a Layer 2 port-mirroring firewall filter action:

1. Enable the configuration of forwarding options.

```
[edit]
user@host set forwarding-options port-mirroring family (inet | inet6) output
```

2. Enable configuration of a next-hop-group for Layer 2 port mirroring.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output]
user@host# set next-hop-group next-hop-group-name
```

3. Specify the type of addresses to be used in the next-hop group configuration.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# set group-type inet6
```


- Specify the interfaces of the next-hop route.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# set interface logical-interface-name-1
user@host# set interface logical-interface-name-2
```

or

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# set interface interface-name next-hop next-hop-address
```

The MX Series router supports up to 30 next-hop groups. Each next-hop group supports up to 16 next-hop addresses. Each next-hop group must specify at least two addresses. The *next-hop-address* can be an IPv4 or IPv6 address.

- (Optional) Specify the next-hop subgroup.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# set next-hop-subgroup subgroup-name interface interface-name next-hop
next-hop-address
```

- Verify the configuration of the next-hop group.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group
next-hop-group-name]
user@host# top
[edit]
user@host# show forwarding-options
```

```
...
next-hop-group next-hop-group-name {
  group-type inet6;
  interface logical-interface-name-1;
  interface interface-name{
    next-hop next-hop-address;
  }
  next-hop-subgroup subgroup-name{
    interface interface-name{
      next-hop next-hop-address;
    }
  }
}
...
```

Related Documentation

- [Configuring Port Mirroring on page 173](#)
- [Example: Multiple Port Mirroring with Next-Hop Groups Configuration on page 191](#)
- [Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices](#)

Example: Multiple Port Mirroring with Next-Hop Groups Configuration

When you need to analyze traffic containing more than one packet type, or you wish to perform multiple types of analysis on a single type of traffic, you can implement multiple

port mirroring and next-hop groups. You can make up to 16 copies of traffic per group and send the traffic to next-hop group members. A maximum of 30 groups can be configured on a router at any given time. The port-mirrored traffic can be sent to any interface, except aggregated SONET/SDH, aggregated Ethernet, loopback (**lo0**), or administrative (**fxp0**) interfaces. To send port-mirrored traffic to multiple flow servers or packet analyzers, you can use the **next-hop-group** statement at the **[edit forwarding-options]** hierarchy level.

Figure 7: Active Flow Monitoring—Multiple Port Mirroring with Next-Hop Groups Topology Diagram

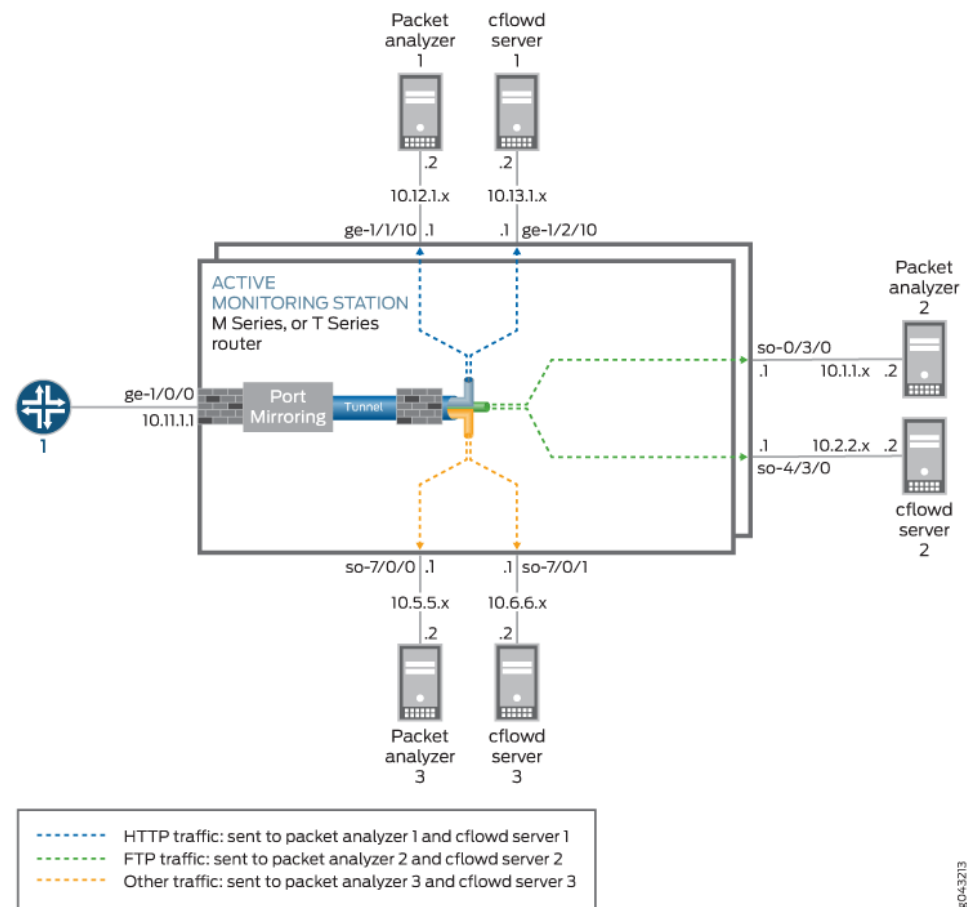


Figure 7 on page 192 shows an example of how to configure multiple port mirroring with next-hop groups. All traffic enters the monitoring router at interface **ge-1/0/0**. A firewall filter counts and port-mirrors all incoming packets to a Tunnel Services PIC. A second filter is applied to the tunnel interface and splits the traffic into three categories: HTTP traffic, FTP traffic, and all other traffic. The three types of traffic are assigned to three separate next-hop groups. Each next-hop group contains a unique pair of exit interfaces that lead to different groups of packet analyzers and flow servers.



NOTE: Instances enabled to mirror packets to different destinations from the same PFE, also use different sampling parameters for each instance. When we configure Layer2 Port-mirroring with both global port-mirroring and instance based port-mirroring, PIC level instances will override FPC level and the FPC level will override the Global instance.

```
[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 10.11.1.1/24;
      }
    }
  }
  ge-1/1/0 { # This is an exit interface for HTTP packets.
    unit 0 {
      family inet {
        address 10.12.1.1/24;
      }
    }
  }
  ge-1/2/0 { # This is an exit interface for HTTP packets.
    unit 0 {
      family inet {
        address 10.13.1.1/24;
      }
    }
  }
  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 10.2.2.1/30;
      }
    }
  }
  so-7/0/0 { # This is an exit interface for all remaining packets.
    unit 0 {
      family inet {
        address 10.5.5.1/30;
      }
    }
  }
}
```

```

so-7/0/1 { # This is an exit interface for all remaining packets.
    unit 0 {
        family inet {
            address 10.6.6.1/30;
        }
    }
}
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.
            }
        }
    }
}
forwarding-options {
    port-mirroring { # This is required when you configure next-hop groups.
        family inet {
            input {
                rate 1; # This port-mirrors all packets (one copy for every packet received).
            }
            output { # Sends traffic to a tunnel interface to enable multipoint 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 so-4/3/0.0; # interface name.
        interface so-0/3/0.0;
    }
    next-hop-group http-traffic { # Configure a next hop for all multipoint interfaces.
        interface ge-1/1/0.0 {
            next-hop 10.12.1.2;
        }
        interface ge-1/2/0.0 {
            next-hop 10.13.1.2;
        }
    }
    next-hop-group default-collect {
        interface so-7/0/0.0;
        interface so-7/0/1.0;
    }
}
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.
                }
            }
        }
    }
}

```

```
    }  
  }  
}  
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 sends all remaining traffic to a final next-hop group.  
    then next-hop-group default-collectors;  
  }  
}  
}
```

- Related Documentation**
- [Understanding Port Mirroring on page 173](#)
 - [Configuring Port Mirroring on page 173](#)

PART 4

Real-Time Performance Monitoring and Video Monitoring Services

- [Monitoring Traffic Using Real-Time Performance Monitoring on page 199](#)
- [Managing License Server for Throughput Data Export on page 223](#)
- [Testing the Performance of Network Devices Using RFC 2544-Based Benchmarking on page 227](#)
- [Tracking Streaming Media Traffic Using Inline Video Monitoring on page 309](#)

CHAPTER 11

Monitoring Traffic Using Real-Time Performance Monitoring

- [Real-Time Performance Monitoring Services Overview on page 199](#)
- [Two-Way Active Measurement Protocol Overview on page 201](#)
- [Configuring RPM Probes on page 201](#)
- [Configuring RPM Receiver Servers on page 206](#)
- [Limiting the Number of Concurrent RPM Probes on page 206](#)
- [Configuring RPM Timestamping on page 207](#)
- [Configuring TWAMP on page 210](#)
- [Configuring BGP Neighbor Discovery Through RPM on page 211](#)
- [Examples: Configuring BGP Neighbor Discovery Through RPM on page 214](#)
- [Tracing RPM Operations on page 215](#)
- [Examples: Configuring Real-Time Performance Monitoring on page 217](#)
- [Enabling RPM for the Services SDK on page 221](#)

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 211](#)
 - [\[edit services rpm\] Hierarchy Level on page 335](#)
 - [Examples: Configuring BGP Neighbor Discovery Through RPM on page 214](#)

Two-Way Active Measurement Protocol Overview

The Two-Way Active Measurement Protocol (TWAMP) is an open protocol for measuring network performance between any two devices supporting the TWAMP protocol. The TWAMP-Control protocol is used to set up performance measurement sessions. The TWAMP-Test protocol is used to send and receive performance measurement probes.

The TWAMP architecture is composed of the following entities that are responsible for starting a monitoring session and exchanging packets:

- The control client initiates all requested test sessions with a start sessions message, and the server acknowledges. When necessary, the control client sends a message to stop all test sessions.
- The session sender and the session reflector exchange test packets according to the TWAMP-Test protocol for each active session. On receiving a TWAMP-Test packet, the session reflector only reflects a measurement packet and does not collect packet statistics in TWAMP.

The TWAMP server is an end system that manages one or more TWAMP sessions and is also capable of configuring per-session ports. The server listens on the TCP port. The session and server make up the TWAMP responder in an IP service-level agreement operation.

TWAMP on MX series routers

For 15.1, both the control client and session sender would be residing on the same Juniper router. The client design does not mandate the server and the session reflector to be on the same system. Hence the Juniper TWAMP client will also be capable of working with a third-party server implementation.

- Related Documentation**
- [post-cli-implicit-firewall on page 463](#)

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 (Services) 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 207), 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.

- 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 207](#). 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 source IPv6 address to be used for RPM probes that are sent from the RPM client (the device that originates the RPM packets) to the RPM server (the device that receives the RPM probes), include the **inet6-options source-address ipv6-address statement** at the **[edit services rpm probe owner test test-name]** hierarchy level. If the source IPv6 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.
- 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) or IP version 6 (IPv6) 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 1 through 86400 seconds.



NOTE: Starting with Junos OS Release 15.1, the minimum period for which the RPM client waits between two tests is modified to be 1 second instead of 0 seconds. Also, if you do not configure the test interval, the default value is 1 second.

- 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.
 - **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 199](#)
- [Examples: Configuring Real-Time Performance Monitoring on page 217](#)

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 (RPM) number;
  }
  udp {
    port (RPM) number;
  }
}
```

The port number specified for the UDP and TCP server can be 7 or from 49160 through 65535.

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.

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, you can enable hardware timestamping of RPM probe messages. The timestamp is applied on both the RPM client router (the router 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.
- SDK Services package on M Series, MX Series, and T Series services PICS that support the Services SDK.
- 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.

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 (Interfaces) (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 AS 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, 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 Series router 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.



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 *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 *Junos OS Routing Protocols Library for Routing Devices*; for more information about queuing, see the *Class of Service Feature Guide for Security Devices*.

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.

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;
    inactivity-timeout seconds;
    maximum-connections count;
    maximum-connections-per-client count;
    maximum-sessions count;
    maximum-sessions-per-connection count;
    port number;
  }
}
```

The TWAMP configuration process includes the following tasks:

- [Configuring TWAMP Interfaces on page 210](#)
- [Configuring TWAMP Servers on page 210](#)

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;
  inactivity-timeout seconds;
  maximum-connections count;
  maximum-connections-per-client count;
  maximum-sessions count;
  maximum-sessions-per-connection count;
  port number;
}
```

- 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 2048 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.
- 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. This statement is mandatory.

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 1 through 86400 seconds.



NOTE: Starting with Junos OS Release 15.1, the minimum period for which the RPM client waits between two tests is modified to be 1 second instead of 0 seconds. Also, if you do not configure the test interval, the default value is 1 second.

- Related Documentation**
- [Real-Time Performance Monitoring Services Overview on page 199](#)
 - [\[edit services rpm\] Hierarchy Level on page 335](#)
 - [Examples: Configuring BGP Neighbor Discovery Through RPM on page 214](#)

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 199](#)
- [Configuring BGP Neighbor Discovery Through RPM on page 211](#)
- [\[edit services rpm\] Hierarchy Level on page 335](#)

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 216](#)
2. [Configuring the Number and Size of RPM Log Files on page 216](#)
3. [Configuring Access to the Log File on page 216](#)
4. [Configuring a Regular Expression for Lines to Be Logged on page 216](#)
5. [Configuring the Trace Operations on page 217](#)

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 26 on page 217 describes the meaning of the RPM tracing flags.

Table 26: RPM Tracing Flags

Flag	Description	Default Setting
all	Trace all operations.	Off
configuration	Trace configuration events.	Off
error	Trace events related to catastrophic errors in daemon.	Off
ipc	Trace IPC events.	Off
ppm	Trace ppm events.	Off
statistics	Trace statistics.	Off

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 199](#)
- [\[edit services rpm\] Hierarchy Level on page 335](#)
- [Examples: Configuring BGP Neighbor Discovery Through RPM on page 214](#)

Enabling RPM for the Services SDK

Real-time performance monitoring (RPM), which has been supported on the adaptive services interface, is now supported by the Services SDK. RPM is supported on all platforms and service PICs that support the Services SDK.

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 199](#)
- [Examples: Configuring Real-Time Performance Monitoring on page 217](#)
- [destination-interface on page 369](#)

Managing License Server for Throughput Data Export

- [License Server Management for Throughput Data Export for NAT, Firewall, and Inline Flow Monitoring Services](#) on page 223
- [Guidelines for Configuring Transmission of Per-Service Throughput to an External Log Collector](#) on page 225

License Server Management for Throughput Data Export for NAT, Firewall, and Inline Flow Monitoring Services

To support Juniper's transition to the Software Defined Networks (SDN), Juniper Networks supports the Software Business Model Transformation, which includes new licensing, pricing, and branding strategies that make it easier for users to extract value from Juniper software solutions. This value of this approach is known as the Juniper Software Advantage (JSA), which provides the following benefits:

- Simple—Simple to buy, use, and manage rights
- Repeatable—License models which facilitates repeatable use among multiple hardware platforms and usage scenarios.
- Measurable—License fees based on easy to measure usage

Although the licensing of JSA products is trust-based, Juniper Networks might periodically audit the usage of its products. License Measurement Tool (LMT) is a technique that is used to compute the usage of individual Network Edge Products under JSA. MX Series routers need to define the mechanism for updating the LMT tool with information such as per-service throughput. For example, for services such as carrier-grade NAT and inline flow monitoring, the router needs to calculate per service throughput and update it in LMT.

On MX Series routers, the Routing Engine periodically sends query messages to every Service PIC on which the service, for which throughput collection is being performed, is configured to run. This polling is performed for all the services for which throughput measurement is enabled. Service PICs, upon receiving the query for a particular service, reply with the throughput measured during the last query interval, for that service. If a service PIC hosts multiple services, the Routing Engine sends separate throughput queries to that service PIC for all the services. If a service is configured on multiple services PICs,

the Routing Engine aggregates the throughput values received from all of them and exports the aggregated throughput to the log collector in the predefined log format. The LMT application analyzes these values from the log collector, performs aggregation on values collected from all routers, and displays them in the LMT application.

You can configure the capability to transmit the throughput details per service for the Junos Address Aware (carrier-grade NAT) and Junos Traffic Vision (previously known as Jflow) in the last time interval to an external log collector. The default time interval at which the throughput data is sent is 300 seconds, which you can configure to suit your network needs. Multiple instances of the same service running on different PICs within a router are supported. If the same service is running on different PICs within a router, the router transmits the consolidated final throughput to the log collector or server. This functionality is supported on MX Series routers with MS-MCPs and MS-MICs, and also in the MX Series Virtual Chassis configuration. To configure the license server properties for throughput data to be transmitted for the defined services, such as NAT or stateful firewall, from the service PIC on the router to the external log collector, include the `license-server` statement at the `[edit]` hierarchy level. To specify the IP address of the license log server, include the `ip-address address` statement at the `[edit license-server]` hierarchy level. To configure the frequency of transmission of throughput data, include the `log-interval seconds` statement at the `[edit license-server]` hierarchy level. To specify the services for which throughput data collection must be performed, include the `services (jflow | cgnat | firewall)` statement at the `[edit license-server]` hierarchy level.

Throughput Measurement and Export

Throughput is defined as: “The network traffic throughput processed by Juniper software in a second. It is represented as Mb/Sec (Megabits per second) or GB/sec (Gigabits per second). Throughput is measured as the 95th percentile of all the peaks measured in a quarter.” Service PICs keep track of the amount of data (in bits) processed by the various service plugins running on them. When a throughput query arrives from RE, for a particular service, the Service PIC returns the value D/T mbps, in its reply, where:

- D is the amount of data (megabits) processed by that service since the previous query was received. If the query interval happens to be 300 seconds, for example, then D refers to the amount of data that was processed during the last 300 second interval. If the current query happens to be the very first query, for a particular service, then D represents the cumulative data bits processed so far, by that service.
- T is the time (seconds) that elapsed since the previous query was received. This is the query interval configured using the CLI interface. If the current query happens to be the very first query, for a particular service, then T represents the time that elapsed since that service started processing packets. For all subsequent queries, T would equal the query interval.

The Routing Engine aggregates the throughput measured (in mbps) across all the Service PICs on which a particular Service is configured and exports it to the Log collector which performs the 95th percentile calculation.

Guidelines for Configuring Transmission of Per-Service Throughput to an External Log Collector

Observe the following guidelines while configuring this functionality on MX Series routers with MS-MPCs and MS-MICs:

- If the syslog server is unreachable, the router cannot send information to the log collector.
- After a graceful Routing Engine switchover (GRES) procedure, the newly functioning active Routing Engine starts sending the data to the server after the configured time interval, which is similar to a reset operation. The time elapsed in the active interval and data before GRES are not preserved.
- The time range must be from 60 through 86400 seconds (24 hours).
- If the timer is not configured, the default value of 300 seconds is assumed.
- The throughput data can be sent only if a service is up and running.
- Only maximum throughput is transmitted for the last 300 seconds or the configured time interval.
- The throughput value must not be less than zero to enable transmission. The data is sent based on the timezone of the router.
- An acknowledgment mechanism for data sent to the log collector is not supported. The router does not receive any acknowledgement regarding whether the data is already written into the log collector.
- The router does not maintain throughput data beyond the configurable time interval.
- No mechanisms exist to track if the log collector is successfully receiving the sent data or if the log server is reachable.
- The time interval and log collector are common for all the services; you cannot configure a different period for collection of logs for each service or a different log collector for each service.
- You cannot clear the system throughput value using a CLI command. It is assumed that the throughput value is not cleared or changed from outside. Throughput must be calculated internally by services and must not be manually modified by a CLI.
- SNMP support for these values is not available.
- The log collector performs a 95 percentile calculation of throughput data. Syslogs are sent even in scaled system conditions to the log collector for the throughput data related to the configured services.
- The following is the format of the syslogs configured to be sent at the prescribed frequency:

```
<Date> <Time> < time-zone> <Router_name> <Service_name> <Throughput_value>
Throughput = <Unit_Mbps/Gbps> in last <Time_Interval>
```

An example is as follows:

Jan 8 08:49:57 America/Adak deuterium CGNAT Throughput = 1500000 Mbps in
last 300Sec

Testing the Performance of Network Devices Using RFC 2544-Based Benchmarking

- [RFC2544-Based Benchmarking Tests Overview on page 227](#)
- [RFC2544-Based Benchmarking Tests for E-LAN and E-Line Services Overview on page 231](#)
- [Supported RFC2544-Based Benchmarking Statements on MX104 Routers on page 234](#)
- [Configuring an RFC 2544-Based Benchmarking Test on page 235](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for Layer 3 IPv4 Services on page 239](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for UNI Direction of Ethernet Pseudowires on page 246](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for NNI Direction of Ethernet Pseudowires on page 254](#)
- [Example: Configuring RFC2544-Based Benchmarking Tests for Layer 2 E-LAN Services in Bridge Domains on page 262](#)
- [Example: Configuring Benchmarking Tests to Measure SLA Parameters for E-LAN Services Using VPLS on page 287](#)

RFC2544-Based Benchmarking Tests Overview

RFC2544 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. These tests are the standard benchmarking tests for Ethernet networks and are known as RFC2544-based benchmarking tests. These tests measure throughput, latency, frame loss rate, and bursty frames. 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 (10 seconds through 1,728,000 seconds), and the frame format (UDP-over-IP).



NOTE: RFC2544-based benchmarking tests support only UDP over IPv4 test traffic (unicast).

An RFC2544-based benchmarking test is performed by transmitting test packets from a device that functions as the generator or the initiator (which is also called the originator). These packets are sent to a device that functions as a reflector, which receives and returns the packets to the initiator.

Juniper Networks MX104 3D Universal Edge Routers support only the reflector function and the corresponding benchmarking tests. Starting from release 15.1, MX104 routers also perform verification of signatures on the received test frames. By default, when the MX104 router receives a test packet that does not have the signature pattern, the packet is dropped. If you generate test traffic using a third-party vendor tool instead of an ACX Series router, you can disable signature verification. To disable signature verification, use the **disable-signature-check** command.

The RFC2544-based benchmarking test 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 27 on page 229](#) describes the different network topologies in which the benchmarking test is supported.

Table 27: Supported Network Topologies for RFC2544 Benchmarking Tests

Service Type	Traffic Direction	Mode	Initial Release on MX104 Routers	Whether the Benchmarking Test Is Supported
E-Line (family bridge)	(UNI) Egress	Port Port, VLAN	14.2R1 (E-Line family bridge)	Supported
E-LAN	(UNI) Egress		14.2R1	Supported
(family bridge and family vpls)			(E-LAN family bridge) 15.1R1 (E-LAN family vpls)	Supported
E-Line (family ccc)	Ingress Egress		13.3R1 (E-Line pseudowire)	Supported
IP Services (family inet)	NNI		13.3R1	Supported



NOTE: You can configure a total of four simultaneous active reflection sessions. The four active reflection sessions can be of the same type or can be a combination of the different types of reflection sessions. For instance, you can configure either four IPv4 reflection sessions or one session each for pseudowire reflection, VPLS reflection, Layer 2 reflection, and IPv4 reflection. The maximum reflection bandwidth supported is 4 Gbps in a standalone test condition.

Table 28 on page 229 lists the interfaces and the reflection type on which the benchmarking tests are supported.

Table 28: Supported Interfaces for RFC2544 Benchmarking Tests

Type of Reflection	Gigabit Interfaces (ge)	Aggregated Interfaces (ae)	10G Interfaces (xe)	Pseudo Interfaces (irb, lt, vt, lo0, and others)
IPv4	Yes	No	No	No
Pseudowire ingress	Yes	No	No	No

Table 28: Supported Interfaces for RFC2544 Benchmarking Tests (*continued*)

Type of Reflection	Gigabit Interfaces (ge)	Aggregated Interfaces (ae)	10G Interfaces (xe)	Pseudo Interfaces (irb, lt, vt, lo0, and others)
Pseudowire egress	Yes	Yes	Yes	No
Layer 2 bridge	Yes	Yes	Yes	No
Layer 2 VPLS	Yes	Yes	Yes	No

All active RFC2544-based benchmarking tests are stopped when any of the following events takes place:

- System events such as Packet Forwarding Engine restarts, Routing Engine restarts, and so on.
- Test interface change events such as deactivation and reactivation of the interface, disabling and enabling of the interface, child link events for aggregated interfaces and so on.

After the benchmarking tests are stopped, the test states of the tests are removed and the user can restart the same test. Other ongoing tests on other interfaces are not interrupted.



NOTE: RFC2544-based benchmarking tests are not supported during unified in-service software upgrade (ISSU) and graceful Routing Engine switchover (GRES).

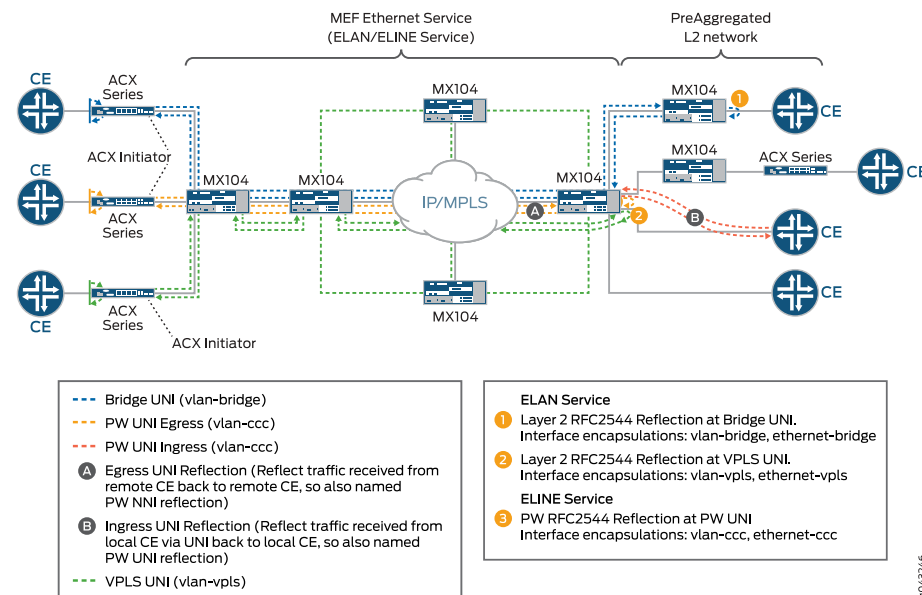
Related Documentation

- [Configuring an RFC 2544-Based Benchmarking Test on page 235](#)
- [Supported RFC2544-Based Benchmarking Statements on MX104 Routers on page 234](#)

RFC2544-Based Benchmarking Tests for E-LAN and E-Line Services Overview

The Metro Ethernet Forum (MEF) defines two Ethernet service types—E-LAN and E-Line—and specifies the associated service attributes and parameters. These services can be supported within the Metro Ethernet Network (MEN) and also supported over different transport technologies such as SONET, MPLS, and so on. Juniper Networks ACX Series routers and MX104 routers provide support for Layer 2 E-LAN and E-Line services reflection. [Figure 8 on page 231](#) shows a sample topology for the E-LAN and E-Line reflection supported on MX104 routers.

Figure 8: E-LAN And E-Line Reflection in a metro Solution



MX104 routers support RFC2544-based benchmarking tests for Layer 2 reflection (E-Line service) by using pseudowires (Layer 2 circuit and L2VPN). E-Line provides transparent data transport. You can configure RFC2544-based benchmarking tests for both ingress and egress direction on the customer edge (CE) facing interface of family type CCC for an Ethernet pseudowire.

MX104 routers support RFC2544-based benchmarking tests for Layer 2 reflection (E-LAN service) by using VPLS and basic bridge domains. VPLS enables geographically dispersed sites to share an Ethernet broadcast domain by connecting sites across an MPLS network. All sites appear to be in the same Ethernet LAN though traffic travels across the MPLS network. Both LDP-based VPLS and BGP-based VPLS are supported. RFC2544-based benchmarking and performance measurement testing for Layer 2 E-LAN services (**bridge/VPLS**) is supported on unicast traffic in egress direction only.

During the benchmarking tests, the initiator or generator transmits a test packet (unicast) to a reflector. The reflector receives and reflects the test packet back to the initiator. The test packet is an UDP-over-IP packet with a source and destination MAC address.

In a E-LAN service, the Layer 2 traffic reflection session is identified by the source MAC address, the destination MAC address, and the egress interface (logical interface). By default, RFC2544-based benchmarking tests are performed when there is no other service traffic. This mode of operation is known as out-of-service mode. The default service mode for the reflecting egress interface for an E-LAN service is also out-of-service mode. In out-of-service mode, while the test is running, all the data traffic (other than test traffic) sent to and from the test interface under test is interrupted. If the test is activated on a logical interface, all the traffic sent to and from the logical interface is interrupted. However, if there are other logical interfaces on the UNI port, the traffic sent to and from those logical interfaces is not interrupted. Control protocol peering is not interrupted whereas pass through control protocol packets such as end-to-end CFM sessions are interrupted. If you do not want the control protocol packets interrupted, you can configure the E-LAN service mode as in-service mode. In the in-service mode, while the test is running, the rest of the data traffic flow sent to and from the UNI port under test on the service is not interrupted. Both peering and pass through control protocols are not interrupted.

In an E-Line service, the reflection session is identified by the egress interface which is the logical interface. On activation of reflection on a logical interface, the traffic received on the logical interface is reflected. You can specify the type of traffic you want reflected by specifying the EtherType (specifies the protocol transported). If you do not specify the EtherType, all traffic is reflected. System does not explicitly block other traffic on the test interface during E-line service. You can block non-test traffic using firewall filters.

By default, for E-LAN services, the reflector swaps MAC addresses. The reflector swaps the source and destination MAC addresses and sends the packet back to the initiator. By default, for E-Line services, the reflector does not swap MAC addresses.

[Table 29 on page 232](#) describes the MAC address swapping behavior for the service types.

Table 29: MAC Address Swapping Behavior for E-LAN and E-Line Services

Family	Direction	Default Behavior	User-configurable
bridge	Egress	MAC address swap (E-LAN service type)	No
		No MAC address swap (E-Line service type)	Yes
vpls	Egress	MAC address swap (E-LAN service type)	No
ccc	Egress	No MAC address swap	Yes
	Ingress	MAC address swap	No

By default, the IP addresses and UDP ports are not modified. Optionally, you can configure the reflector to swap the source and destination IP address and the source and destination UDP ports.

You can configure an ACX Series router to operate as an initiator as well as a reflector. The MX104 router can be configured to operate only as a reflector.

MX104 routers also support the specification of the protocol transported in the Ethernet frame. To specify the EtherType (specifies the protocol transported) used for reflection of the test frames, use the **reflect-etype** command. If you do not specify the EtherType, all EtherTypes are reflected.



NOTE: The maximum reflection bandwidth supported is 4 Gbps. Because RFC2544 reflection shares system bandwidth with other loopback services such as tunnel services, you must manage the sharing of bandwidth for performing RFC2544-based performance tests.



NOTE: RFC2544-based benchmarking tests are not supported during unified in-service software upgrade (ISSU) and graceful Routing Engine switchover (GRES).

**Related
Documentation**

- [RFC2544-Based Benchmarking Tests Overview on page 227](#)
- [Supported RFC2544-Based Benchmarking Statements on MX104 Routers on page 234](#)
- [Example: Configuring RFC2544-Based Benchmarking Tests for Layer 2 E-LAN Services in Bridge Domains on page 262](#)
- [disable-signature-check on page 377](#)
- [reflect-etype on page 474](#)

Supported RFC2544-Based Benchmarking Statements on MX104 Routers

Table 30 on page 234 lists the reflector-specific configuration statements that are supported on the MX104 routers. Note that en dash (–) specified in the Initial Release on MX104 Routers column denotes that the command is not supported.

Table 30: Supported RFC2544-Based Benchmarking Reflector Statements on MX104

Statement	Options	Initial Release on MX104 Routers
<code>destination-ipv4-address</code>	–	13.3R1
<code>destination-mac-address</code>	–	14.2R1
<code>destination-udp-port</code>	–	13.3R1
<code>direction</code>	(egress ingress)	13.3R1
<code>disable-signature-check</code>	–	15.1R1
<code>family</code>	(ccc inet)	13.3R1
	(bridge ccc inet)	14.2R1
	(vpls)	15.1R1
<code>in-service</code>	–	14.2R1
<code>ip-swap</code>	–	14.2R1
<code>mode</code>	reflect	13.3R1
<code>reflect-etype</code>	–	15.1R1
<code>reflect-mode</code>	(mac-swap no-mac-swap)	14.2R1
<code>service-type</code>	(eline elan)	14.2R1
<code>source-ipv4-address</code>	–	13.3R1
<code>source-mac-address</code>	–	14.2R1
<code>source-udp-port</code>	–	13.3R1
<code>test-interface</code>	–	13.3R1
<code>udp-tcp-port-swap</code>	–	14.2R1

- Related Documentation**
- [RFC2544-Based Benchmarking Tests Overview on page 227](#)
 - [Configuring an RFC 2544-Based Benchmarking Test on page 235](#)

- [Example: Configuring RFC2544-Based Benchmarking Tests for Layer 2 E-LAN Services in Bridge Domains on page 262](#)

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.



NOTE: The test configuration is applied only when you start the test. If you update the test configuration during the test, you have to start the test again for the updated configuration to take effect.

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.

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, Ethernet pseudowire, and Layer 2 bridge networks:

- [Configuring a Test Name for an RFC 2544-Based Benchmarking Test for a IPv4 Network on page 235](#)
- [Configuring a Test Name for an RFC 2544-Based Benchmarking Test for an Ethernet Pseudowire on page 237](#)
- [Configuring a Test Name for an RFC 2544-Based Benchmarking Test for a Layer 2 E-LAN Service in Bridge Domain on page 238](#)

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
```

Configuring a Test Name for an RFC 2544-Based Benchmarking Test for a Layer 2 E-LAN Service in Bridge Domain

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 (bridge), 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 a layer 2 E-LAN service in Bridge domains:

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, l2b-test1. The test name identifier can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name l2b-test1
```

5. Specify the source and destination MAC addresses of the test packet. Both these parameters are valid only for the bridge family.

```
[edit services rpm rfc2544-benchmarking tests test-name l2b-test1]
user@host# set source-mac-address address destination-mac-address address
```

6. Specify the service type under test. This parameter is applicable only for the bridge family.

```
[edit services rpm rfc2544-benchmarking tests test-name l2b-test1]
user@host# set service-type elan
```


7. Specify the test mode for the packets that are sent during the benchmarking test. The **reflect** option causes the test frames to be reflected over the Layer 2 bridge.

```
[edit services rpm rfc2544-benchmarking tests test-name l2b-test1]
user@host# set mode reflect
```

8. Configure the address type family for the benchmarking test. The **bridge** option indicates that the test is run on a E-LAN service over a bridge domain.

```
[edit services rpm rfc2544-benchmarking tests test-name l2b-test1]
user@host# set family bridge
```

9. 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 l2b-test1]
user@host# set direction egress
```

10. Specify the logical interface on which the RFC 2544-based benchmarking test is run.

```
[edit services rpm rfc2544-benchmarking tests test-name l2b-test1]
user@host# set test-interface interface-name
```

Related Documentation

- [RFC2544-Based Benchmarking Tests Overview on page 227](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for UNI Direction of Ethernet Pseudowires on page 246](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for NNI Direction of Ethernet Pseudowires on page 254](#)
- [Example: Configuring RFC2544-Based Benchmarking Tests for Layer 2 E-LAN Services in Bridge Domains on page 262](#)
- [Example: Configuring an RFC 2544-Based Benchmarking Test for Layer 3 IPv4 Services on page 239](#)

Example: Configuring an RFC 2544-Based Benchmarking Test for Layer 3 IPv4 Services

- [Requirements on page 239](#)
- [Overview on page 240](#)
- [Configuration on page 240](#)
- [Verifying the Results of the Benchmarking Test for Layer 3 IPv4 Services on page 246](#)

Requirements

This example uses the following hardware and software components:

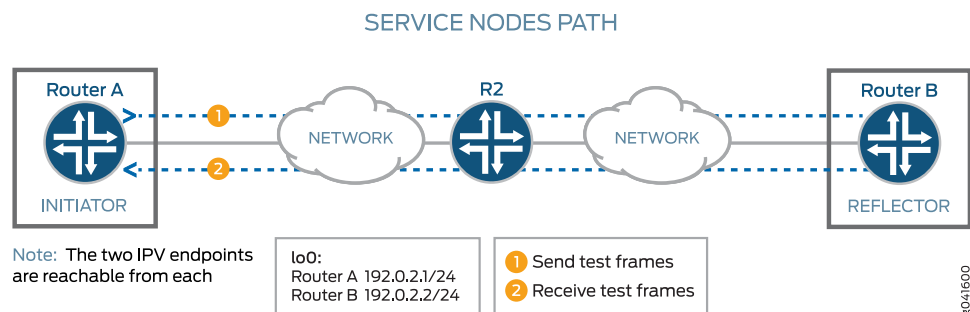
- An ACX Series Universal Access Router
- Junos OS Release 13.3 or later

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 9 on page 240 shows the sample topology to perform an RFC 2544 test for a Layer 3 IPv4 Service.

Figure 9: 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 241](#)
- [Configuring Benchmarking Test Parameters on Router B on page 243](#)
- [Results on page 245](#)

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@host> 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 246](#)

---

### 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>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li></ul>                                                                                                                                                                   |

---

## 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 247](#)
- [Overview on page 247](#)



- [Configuration on page 248](#)
- [Verifying the Results of the Benchmarking Test for UNI Direction of an Ethernet Pseudowire Service on page 254](#)

## Requirements

This example uses the following hardware and software components:

- An ACX Series router
- Junos OS Release 13.3 or later

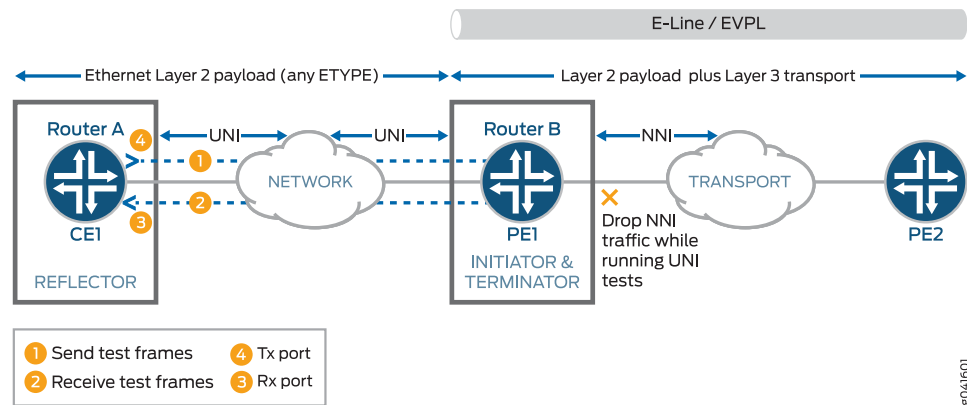
## Overview

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 10 on page 248](#) shows the sample topology to perform an RFC 2544 test for the UNI direction of an Ethernet pseudowire service.

Figure 10: 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 249](#)
- [Configuring Benchmarking Test Parameters on Router B on page 251](#)
- [Results on page 253](#)

### 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
```
16. 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 stop** 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 {
 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 254](#)

---

### 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="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li></ul>                                                                                                                                                                   |

---

## 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 255](#)
- [Overview on page 255](#)
- [Configuration on page 256](#)
- [Verifying the Results of the Benchmarking Test for NNI Direction of an Ethernet Pseudowire Service on page 262](#)



## Requirements

This example uses the following hardware and software components:

- An ACX Series Universal Access Router
- Junos OS Release 13.3 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).

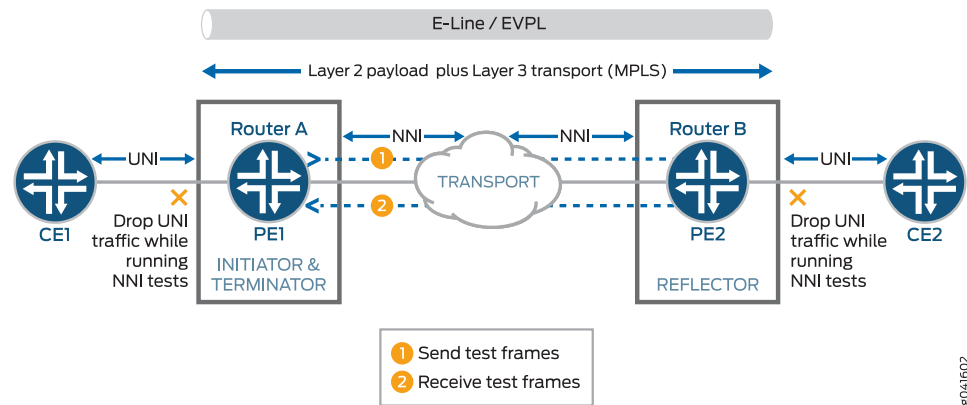


**NOTE:** When pseudowire reflection is enabled on an interface, the router does not block the ingress or egress traffic through the test interface. To block other data traffic, you must explicitly configure firewall filters.

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 11 on page 256](#) shows the sample topology to perform an RFC 2544 test for the NNI direction of an Ethernet pseudowire service.

Figure 11: 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 A on page 257](#)
- [Configuring Benchmarking Test Parameters on Router B on page 259](#)
- [Results on page 261](#)

### 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
```



**NOTE:** When pseudowire reflection is enabled on an interface, the router does not block the ingress or egress traffic through the test interface. To block other data traffic, you must explicitly configure firewall filters.

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
```

16. 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 stop** 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 {
 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 262](#)

---

### 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="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li></ul>                                                                                                                                                                   |

---

## Example: Configuring RFC2544-Based Benchmarking Tests for Layer 2 E-LAN Services in Bridge Domains

This example shows how to configure benchmarking tests for the Layer 2 E-LAN services in bridge domains. The example covers the four basic tests: throughput, frame-loss, back-to-back, and latency.

- [Requirements on page 263](#)
- [Overview on page 263](#)
- [Configuration on page 264](#)
- [Verifying the Results of the Benchmarking Tests for Layer 2 Services \(E-LAN\) in Bridge Domains on page 277](#)



## Requirements

This example uses the following hardware and software components:

- An MX104 3D Universal Edge router
- An ACX Series router
- Junos OS Release 14.2 or later for MX Series routers

## Overview

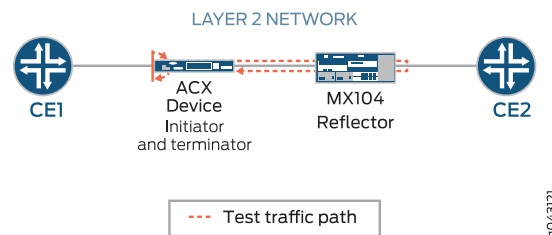
Consider a sample topology in which an ACX router functions as an initiator and terminator of the test frames for an RFC2544-based benchmarking test. ACX router is connected to a customer edge device CE1, on one side and is connected over a Layer 2 network to an MX104 router. The MX104 router functions as a reflector to reflect the test frames it receives from the ACX Series initiator back to the initiator. The MX04 router is also connected to a customer edge device CE2.



**NOTE:** When Layer 2 reflection is enabled on an interface, filters are configured internally to block the ingress and egress traffic except test traffic through the test interface.

Figure 12 on page 263 shows the sample topology to perform all four RFC2544-based benchmarking tests (throughput, back-to-back frames, latency, and frame-loss) for the UNI direction on a Layer 2 bridge network.

**Figure 12: Layer 2 reflection Simple Topology**



On the ACX router, ge-1/2/1.0 is the Layer 2 NNI interface and ge-1/1/3.0 is the Layer 2 UNI interface. On the MX104 router, ge-1/1/6.0 is the Layer 2 NNI interface and ge-1/1/5.0 is the Layer 2 UNI interface. The benchmarking tests are used to compute the performance attributes for an E-LAN service on a bridge domain.



**NOTE:** Test packets can be identified using the destination MAC address, source MAC address, and test interface. Both tagged and untagged interfaces are supported. For tagged interfaces, the test interface is the VLAN sub interface. For untagged interfaces, the physical port represents the test interface. Traffic through other VLAN sub interfaces, present in the same physical port, is not affected when you configure the benchmarking test on one of the sub interfaces.

## Configuration

In this example, you configure the benchmarking tests for the UNI direction for an E-LAN service on a Layer 2 bridge domain that is enabled between two routers to detect and analyze the performance of the interconnected routers. In this example, we start by configuring the ACX Series router. On the ACX router, you first configure each test by specifying the test profile, the test attributes, and then define the test by associating the test with the test profile with the relevant attributes. You can then configure the interface. On the MX104 router, you will perform the same steps. However, a few attributes such as the outer VLAN ID, source UDP port, destination UDP port, the duration of each iteration, and their values are only applicable to the initiator or the ACX router.



**NOTE:** When you configure the Layer 2 reflection, you can specify the service type under test as ELINE if you want to simulate an ELINE service using bridge encapsulation.

- [Configuring Throughput Benchmarking Test Parameters on the ACX Series Router on page 267](#)
- [Configuring Back-to-Back Frames Benchmarking Test Parameters on the ACX Series Router on page 268](#)
- [Configuring Latency Benchmarking Test Parameters on the ACX Series Router on page 269](#)
- [Configuring Frame Loss Benchmarking Test Parameters on the ACX Series Router on page 271](#)
- [Configuring Other Benchmarking Test Parameters on the ACX Series Router on page 272](#)
- [Configuring Benchmarking Test Parameters on the MX104 Router on page 273](#)
- [Configuring Other Benchmarking Test Parameters on the MX104 Router on page 274](#)
- [Results on page 275](#)

### 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

```
set services rpm rfc2544-benchmarking profiles test-profile tput test-type throughput
set services rpm rfc2544-benchmarking profiles test-profile tput packet-size 128
set services rpm rfc2544-benchmarking profiles test-profile tput bandwidth-kbps 900000
```

## Parameters on the ACX Series Router

```

set services rpm rfc2544-benchmarking profiles test-profile b2bt test-type
back-back-frames
set services rpm rfc2544-benchmarking profiles test-profile b2bt packet-size 512
set services rpm rfc2544-benchmarking profiles test-profile b2bt bandwidth-kbps 950000
set services rpm rfc2544-benchmarking profiles test-profile lty test-type latency
set services rpm rfc2544-benchmarking profiles test-profile lty packet-size 512
set services rpm rfc2544-benchmarking profiles test-profile lty bandwidth-kbps 1000000
set services rpm rfc2544-benchmarking profiles test-profile frloss test-type frame-loss
set services rpm rfc2544-benchmarking profiles test-profile frloss packet-size 1600
set services rpm rfc2544-benchmarking profiles test-profile frloss bandwidth-kbps
1000000
set services rpm rfc2544-benchmarking tests test-name tput-test test-profile tput
set services rpm rfc2544-benchmarking tests test-name tput-test source-mac-address
00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name tput-test destination-mac-address
00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name tput-test ovlan-id 400
set services rpm rfc2544-benchmarking tests test-name tput-test service-type elan
set services rpm rfc2544-benchmarking tests test-name tput-test mode
initiate-and-terminate
set services rpm rfc2544-benchmarking tests test-name tput-test family bridge
set services rpm rfc2544-benchmarking tests test-name tput-test direction egress
set services rpm rfc2544-benchmarking tests test-name tput-test source-udp-port 200
set services rpm rfc2544-benchmarking tests test-name tput-test destination-udp-port
200
set services rpm rfc2544-benchmarking tests test-name tput-test test-iterator-duration
20
set services rpm rfc2544-benchmarking tests test-name tput-test test-interface ge-1/1/3.0
set services rpm rfc2544-benchmarking tests test-name b2b-test test-profile b2bt
set services rpm rfc2544-benchmarking tests test-name b2b-test source-mac-address
00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name b2b-test destination-mac-address
00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name b2b-test ovlan-id 400
set services rpm rfc2544-benchmarking tests test-name b2b-test service-type elan
set services rpm rfc2544-benchmarking tests test-name b2b-test mode
initiate-and-terminate
set services rpm rfc2544-benchmarking tests test-name b2b-test family bridge
set services rpm rfc2544-benchmarking tests test-name b2b-test direction egress
set services rpm rfc2544-benchmarking tests test-name b2b-test test-iterator-duration
20
set services rpm rfc2544-benchmarking tests test-name b2b-test test-interface ge-1/1/3.0
set services rpm rfc2544-benchmarking tests test-name lty-test test-profile lty
set services rpm rfc2544-benchmarking tests test-name lty-test source-mac-address
00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name lty-test destination-mac-address
00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name lty-test ovlan-id 400
set services rpm rfc2544-benchmarking tests test-name lty-test service-type elan
set services rpm rfc2544-benchmarking tests test-name lty-test mode
initiate-and-terminate
set services rpm rfc2544-benchmarking tests test-name lty-test family bridge
set services rpm rfc2544-benchmarking tests test-name lty-test direction egress
set services rpm rfc2544-benchmarking tests test-name lty-test source-udp-port 200
set services rpm rfc2544-benchmarking tests test-name lty-test destination-udp-port
200

```

```

set services rpm rfc2544-benchmarking tests test-name lty-test test-iterator-duration 20
set services rpm rfc2544-benchmarking tests test-name lty-test test-interface ge-1/1/3.0
set services rpm rfc2544-benchmarking tests test-name frloss-test test-profile frloss
set services rpm rfc2544-benchmarking tests test-name frloss-test source-mac-address
 00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name frloss-test
 destination-mac-address 00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name frloss-test ovlan-id 400
set services rpm rfc2544-benchmarking tests test-name frloss-test service-type elan
set services rpm rfc2544-benchmarking tests test-name frloss-test mode
 initiate-and-terminate
set services rpm rfc2544-benchmarking tests test-name frloss-test family bridge
set services rpm rfc2544-benchmarking tests test-name frloss-test direction egress
set services rpm rfc2544-benchmarking tests test-name frloss-test source-udp-port 200
set services rpm rfc2544-benchmarking tests test-name frloss-test destination-udp-port
 200
set services rpm rfc2544-benchmarking tests test-name frloss-test test-iterator-duration
 20
set services rpm rfc2544-benchmarking tests test-name frloss-test test-interface ge-1/1/3.0
set interfaces ge-1/2/1 flexible-vlan-tagging
set interfaces ge-1/2/1 mtu 9192
set interfaces ge-1/2/1 encapsulation flexible-ethernet-services
set interfaces ge-1/2/1 unit 0 encapsulation vlan-bridge
set interfaces ge-1/2/1 unit 0 vlan-id 400
set interfaces ge-1/1/3 flexible-vlan-tagging
set interfaces ge-1/1/3 mtu 9192
set interfaces ge-1/1/3 encapsulation flexible-ethernet-services
set interfaces ge-1/1/3 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/3 unit 0 vlan-id 400
set bridge-domains bd1 vlan-id 600
set bridge-domains bd1 interface ge-1/2/1.0
set bridge-domains bd1 interface ge-1/1/3.0

```

#### Configuring Benchmarking Test Parameters on the MX104 Router

```

set services rpm rfc2544-benchmarking tests test-name l2b-reflector source-mac-address
 00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name l2b-reflector
 destination-mac-address 00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name l2b-reflector service-type elan
set services rpm rfc2544-benchmarking tests test-name l2b-reflector mode reflect
set services rpm rfc2544-benchmarking tests test-name l2b-reflector family bridge
set services rpm rfc2544-benchmarking tests test-name l2b-reflector direction egress
set services rpm rfc2544-benchmarking tests test-name l2b-reflector test-interface
 ge-1/1/5.0
set interfaces ge-1/1/6 flexible-vlan-tagging
set interfaces ge-1/1/6 mtu 9192
set interfaces ge-1/1/6 encapsulation flexible-ethernet-services
set interfaces ge-1/1/6 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/6 unit 0 vlan-id 400
set interfaces ge-1/1/5 flexible-vlan-tagging
set interfaces ge-1/1/5 mtu 9192
set interfaces ge-1/1/5 encapsulation flexible-ethernet-services
set interfaces ge-1/1/5 unit 0 encapsulation vlan-bridge
set interfaces ge-1/1/5 unit 0 vlan-id 400
set bridge-domains bd1 domain-type bridge
set bridge-domains bd1 vlan-id 500
set bridge-domains bd1 interface ge-1/1/6.0

```

```
set bridge-domains bd1 interface ge-1/1/5.0
```

### Configuring Throughput Benchmarking Test Parameters on the ACX Series Router

#### Step-by-Step Procedure

The following configuration requires you to configure a test profile for the throughput test and reference the test-profile in a unique test-name. The test-name defines the parameters for the throughput test to be performed on the ACX router.

To configure the throughput test parameters on the ACX Router:

1. In configuration mode, at the `[edit]` hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```

2. Define a name for the first test profile—for example, `tput` for the throughput test profile.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit profiles test-profile tput
```

3. Configure the type of test to be performed as throughput, specify the packet size as 128 bytes, and define the theoretical maximum bandwidth for the test in kilobits per second (Kbps), with a value from 1 Kbps through 1,000,000 Kbps.

```
[edit services rpm rfc2544-benchmarking profiles test-profile tput]
user@host# set test-type throughput packet-size 128 bandwidth-kbps 900000
```

4. Enter the `up` command twice to go to the `[edit services rpm rfc2544-benchmarking]` level in the configuration hierarchy.

```
[edit services rpm rfc2544-benchmarking profiles test-profile tput]
user@host# up
user@host# up
```

5. Define a name for the throughput test—for example, `tput-test`. The test name can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name tput-test
```

6. Specify the name of the test profile, `tput`, to be associated with the test name.

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set test-profile tput
```

7. Configure the source and destination MAC address for the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address
00:00:00:00:22:22
```

8. Configure the outer VLAN ID for the test frames and specify the service type under test to be E-LAN.

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set ovlan-id 400 service-type elan
```

9. 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 tput-test]
user@host# set mode initiate-and-terminate
```

10. Configure the family type, **bridge**, for the benchmarking test and specify the direction, egress. Also, specify the source and destination UDP port to be used in the UDP headers of the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set family bridge direction egress source-udp-port 200
destination-udp-port 200
```

11. Specify the duration of each iteration in seconds, with a value from 10 seconds to 1,728,000 seconds, and specify the logical interface, ge-0/2/1.0, on which the RFC2544-benchmarking tests are run.

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set test-iterator-duration 20 test-interface ge-1/1/3.0
```

### Configuring Back-to-Back Frames Benchmarking Test Parameters on the ACX Series Router

---

#### Step-by-Step Procedure

The following configuration requires you to configure a test profile for the back to back frames test and reference the test-profile in a unique test-name. The test-name defines the parameters for the back to back frames test to be performed on the ACX router.

To configure the back-to-back frames test parameters on the ACX Router:

1. In configuration mode, at the **[edit]** hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```

2. Define a name for the back-to-back test profile—for example, b2bt.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit profiles test-profile b2bt
```

3. Configure the type of test to be performed as back-to-back frames, specify the packet size as 128 bytes, and 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 b2bt]
user@host# set test-type back-to-back-frames packet-size 4444 bandwidth-kbps
950000
```

4. Enter the **up** command twice to go to the **[edit services rpm rfc2544-benchmarking]** level in the configuration hierarchy.

```
[edit services rpm rfc2544-benchmarking profiles test-profile b2bt]
user@host# up
user@host# up
```

5. Define a name for the back-to-back frames test—for example, b2bt-test. The test name can be up to 32 characters in length.  

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name b2bt-test
```
6. Specify the name of the test profile, b2bt, to be associated with the test name.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set test-profile b2bt
```
7. Configure the source and destination MAC address for the test packet.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address
00:00:00:00:22:22
```
8. Configure the outer VLAN ID for the test frames and specify the service type under test.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set ovlan-id 400 service-type elan
```
9. 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 b2bt-test]
user@host# set mode initiate-and-terminate
```
10. Configure the family type, **bridge**, for the benchmarking test and specify the direction, egress.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set family bridge direction egress
```
11. Specify the duration of each iteration in seconds, with a value from 10 seconds to 1,728,000 seconds. Also, specify the logical interface, ge-0/2/1.0, on which the RFC2544-based benchmarking test is run.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set test-iterator-duration 20 test-interface ge-1/1/3.0
```

### Configuring Latency Benchmarking Test Parameters on the ACX Series Router

#### Step-by-Step Procedure

The following configuration requires you to configure a test profile for the latency test and reference the test-profile in a unique test-name. The test-name defines the parameters for the latency test to be performed on the ACX router.

To configure the latency test parameters on the ACX Router:

1. In configuration mode, at the **[edit]** hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.  

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```
2. Define a name for the latency test profile—for example, lty.  

```
[edit services rpm rfc2544-benchmarking]
```

```
user@host# edit profiles test-profile lty
```

3. Configure the type of test to be performed as latency, specify the packet size of the test packet, and define the 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]
```

```
user@host# set test-profile lty test-type latency packet-size 512 bandwidth-kbps 1000000
```

4. Enter the **up** command twice to go to the previous level in the configuration hierarchy.

```
[edit services rpm rfc2544-benchmarking profiles test-profile lty]
```

```
user@host# up
```

```
user@host# up
```

5. Define a name for the latency test—for example, lty-test. The test name can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
```

```
user@host# edit tests test-name lty-test
```

6. Specify the name of the test profile, lty, to be associated with the test name.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set test-profile lty
```

7. Configure the source and destination MAC address for the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address 00:00:00:00:22:22
```

8. Configure the outer VLAN ID for the test frames and specify the service type under test.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set ovlan-id 400 service-type elan
```

9. 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 lty-test]
```

```
user@host# set mode initiate-and-terminate
```

10. Configure the family type, **bridge**, for the benchmarking test and specify the direction, egress. Also, specify the source and destination UDP port to be used in the UDP headers of the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set family bridge direction egress source-udp-port 200 destination-udp-port 200
```

11. Specify the duration of each iteration in seconds, with a value from 10 seconds to 1,728,000 seconds. Also, specify the logical interface, ge-0/2/1.0, on which the RFC2544-based benchmarking test is run.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set test-iterator-duration 20 test-interface ge-1/1/3.0
```



### Configuring Frame Loss Benchmarking Test Parameters on the ACX Series Router

#### Step-by-Step Procedure

The following configuration requires you to configure a test profile for the frame loss test and reference the test-profile in a unique test-name. The test-name defines the parameters for the frame loss test to be performed on the ACX router.

To configure the frame loss test parameters on the ACX Router:

1. In configuration mode, at the **[edit]** hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```

2. Define a name for the frame loss test profile—for example, `frloss`.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit profiles test-profile frloss
```

3. Configure the type of test performed as frame loss, specify the packet size of the test packet, and define the 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]
user@host# set test-profile frloss test-type frame-loss packet-size 1600
bandwidth-kbps 1000000
```

4. Enter the **up** command to go to the previous level in the configuration hierarchy.

```
[edit services rpm rfc2544-benchmarking profiles]
user@host# up
```

5. Define a name for the frame loss test—for example, `frloss-test`. The test name can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name frloss-test
```

6. Specify the name of the test profile, `frloss`, to be associated with the test name.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set test-profile frloss
```

7. Configure the source and destination MAC address for the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address
00:00:00:00:22:22
```

8. Configure the outer VLAN ID for the test frames and specify the service type under test.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set ovlan-id 400 service-type elan
```

9. 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 frloss-test]
```

```
user@host# set mode initiate-and-terminate
```

10. Configure the family type, **bridge**, for the benchmarking test and specify the direction, egress. Also, specify the source and destination UDP port to be used in the UDP headers of the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set family bridge direction egress source-udp-port 200
destination-udp-port 200
```

11. Specify the duration of each iteration in seconds, with a value from 10 seconds to 1,728,000 seconds. Also, specify the logical interface, ge-0/2/1.0, on which the RFC2544-based benchmarking test is run.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set test-iterator-duration 20 test-interface ge-1/1/3.0
```

12. Enter the **exit** command to go to the [edit] hierarchy level.

```
[edit services rpm rfc2544-benchmarking tests test-name test4]
user@host# exit
```

### Configuring Other Benchmarking Test Parameters on the ACX Series Router

---

#### 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*.

To configure the interface and bridge domain on the ACX Router:

1. Configure the Layer 2 NNI interface on which the tests must be run from the **[edit]** hierarchy level.

```
[edit]
user@host# edit interfaces ge-1/2/1
```

2. Configure flexible VLAN tagging for the transmission of untagged frames or 802.1Q single-tagged and dual-tagged frames on the logical interface. You can also specify the maximum transmission unit (MTU) size for the interface and the encapsulation.

```
[edit interfaces ge-1/2/1]
user@host# set flexible-vlan-tagging mtu 9192 encapsulation
flexible-ethernet-services
```

3. Configure a logical unit for the interface, specify the encapsulation, and configure the VLAN ID on the logical interfaces.

```
[edit interfaces ge-1/2/1]
user@host# set unit 0 encapsulation vlan-bridge vlan-id 400
```

4. Configure the Layer 2 UNI interface.

```
[edit]
user@host# edit interfaces ge-1/1/3
```

5. Configure flexible VLAN tagging for transmission of non-tagged frames or 802.1Q single-tag and dual-tag frames on the logical interface. You can also specify the maximum transmission unit (MTU) size for the interface and the encapsulation.

```
[edit interfaces ge-1/1/3]
user@host# set flexible-vlan-tagging mtu 9192 encapsulation
flexible-ethernet-services
```

6. Configure a logical unit for the interface and specify the encapsulation and configure the VLAN ID on the logical interfaces.

```
[edit interfaces ge-1/1/3]
user@host# set unit 0 encapsulation vlan-bridge vlan-id 400
```

7. Configure the bridge domain, bd1, and specify the VLAN ID associated with the bridge domain and the associated interfaces from the [edit] hierarchy level.

```
[edit]
user@host# set bridge-domains bd1 vlan-id 600 interface ge-1/2/1.0
user@host# set bridge-domains bd1 vlan-id 600 interface ge-1/1/3.0
```

### Configuring Benchmarking Test Parameters on the MX104 Router

#### Step-by-Step Procedure

The following configuration requires you to configure a unique test-name for the benchmarking test on the MX104 router. The test-name defines the parameters for the benchmarking test to be performed. Because the test interface and test MAC addresses are the same, you can create a single test configuration at the reflector (MX104).

To configure the benchmarking test parameters on the MX104 Router:

1. In configuration mode, at the [edit] hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```

2. Define a name for the test—for example, l2b-reflector. The test name can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name l2b-reflector
```

3. Specify the source and destination MAC addresses of the test packet.

```
[edit services rpm rfc2544-benchmarking test-name l2b-reflector]
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address
00:00:00:00:22:22
```

4. Specify the service type under test and the mode which is reflect, at the reflector.

```
[edit services rpm rfc2544-benchmarking test-name l2b-reflector]
user@host# set service-type elan
```

5. Specify the mode which is reflect at the reflector.

```
[edit services rpm rfc2544-benchmarking test-name l2b-reflector]
user@host# set mode reflect
```

6. Configure the family type, **bridge** and specify the direction, egress, for the benchmarking test. Also, specify the logical interface, ge-1/1/5.0, on which the RFC2544-based benchmarking test is being run.

```
[edit services rpm rfc2544-benchmarking tests test-name l2b-reflector]
```

```
user@host# set family bridge direction egress test-interface ge-1/1/5.0
```

### Configuring Other Benchmarking Test Parameters on the MX104 Router

**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*.

To configure the interface and bridge domain on the MX104 Router:

1. Configure the Layer 2 NNI interface on which the tests must be run.  

```
[edit]
user@host# edit interfaces ge-1/1/6
```
2. Configure flexible VLAN tagging for transmission of untagged frames or 802.1Q single-tagged and dual-tagged frames on the logical interface. You can also specify the maximum transmission unit (MTU) size for the interface and the encapsulation.  

```
[edit interfaces ge-1/1/6]
user@host# set flexible-vlan-tagging mtu 9192 encapsulation
flexible-ethernet-services
```
3. Configure a logical unit for the interface, specify the encapsulation, and configure the VLAN ID on the logical interface.  

```
[edit interfaces ge-1/1/6]
user@host# set unit 0 encapsulation vlan-bridge vlan-id 400
```
4. Configure the Layer 2 NNI interface.  

```
[edit]
user@host# edit interfaces ge-1/1/5
```
5. Configure flexible VLAN tagging for transmission of untagged frames or 802.1Q single-tagged and dual-tagged frames on the logical interface. You can also specify the maximum transmission unit (MTU) size for the interface and the encapsulation.  

```
[edit interfaces ge-1/1/5]
user@host# set flexible-vlan-tagging mtu 9192 encapsulation
flexible-ethernet-services
```
6. Configure a logical unit for the interface, specify the encapsulation, and configure the VLAN ID on the logical interfaces.  

```
[edit interfaces ge-1/1/5]
user@host# set unit 0 encapsulation vlan-bridge vlan-id 400
```
7. Configure the bridge domain, bd1, and specify the VLAN ID associated with the bridge domain, and the associated interfaces from the [edit] hierarchy level.  

```
[edit]
user@host# set bridge-domains bd1 vlan-id 500 interface ge-1/1/6.0
user@host# set bridge-domains bd1 vlan-id 500 interface ge-1/1/5.0
```
8. Start the benchmarking test on the reflector.  

```
user@host> test services rpm rfc2544-benchmarking test l2b-reflector 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 l2b-reflector stop** command.

## Results

In configuration mode, confirm your configuration on the ACX Router and the MX104 Router 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 the ACX Router :

```
[edit interfaces]
ge-1/2/1 {
 flexible-vlan-tagging;
 mtu 9192;
 encapsulation flexible-ethernet-services;
 unit 0 {
 encapsulation vlan-bridge;
 vlan-id 400;
 }
}
ge-1/1/3 {
 flexible-vlan-tagging;
 mtu 9192;
 encapsulation flexible-ethernet-services;
 unit 0 {
 encapsulation vlan-bridge;
 vlan-id 400;
 }
}

[edit bridge-domains]
bd1 {
 vlan-id 600;
 interface ge-1/2/1.0;
 interface ge-1/1/3.0;
}

[edit services rpm]
rfc2544-benchmarking {
 profiles {
 test-profile tput {
 test-type throughput
 packet-size 128;
 bandwidth-kbps 900000;
 }
 test-profile b2bt {
 test-type back-back-frames
 packet-size 512;
 bandwidth-kbps 950000;
 }
 test-profile lty {
 test-type latency
 packet-size 512;
 bandwidth-kbps 100000;
 }
 test-profile frloss {
 test-type frameloss

```

```
 packet-size 1600;
 bandwidth-kbps 1000000;
 }
}

tests {
 test-name tput-test {
 interface ge-1/1/3.0;
 test-profile tput;
 mode initiate,terminate;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 ovlan-id 400;
 service-type elan;
 family bridge;
 direction egress;
 source-udp-port 200;
 destination-udp-port 200;
 test-iterator-duration 20;
 }
 test-name b2b-test {
 interface ge-1/1/3.0;
 test-profile b2bt;
 mode initiate,terminate;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 ovlan-id 400;
 service-type elan;
 family bridge;
 direction egress;
 test-iterator-duration 20;
 }
 test-name lty-test {
 interface ge-1/1/3.0;
 test-profile lty;
 mode initiate,terminate;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 ovlan-id 400;
 service-type elan;
 family bridge;
 direction egress;
 source-udp-port 200;
 destination-udp-port 200;
 test-iterator-duration 20;
 }
 test-name frloss-test {
 interface ge-1/1/3.0;
 test-profile frloss;
 mode initiate,terminate;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 ovlan-id 400;
 service-type elan;
 family bridge;
 direction egress;
 source-udp-port 200;
 destination-udp-port 200;
 test-iterator-duration 20;
 }
}
```

```
 }
}
```

Benchmarking Test Parameters on the MX104 Router:

```
[edit interfaces]
ge-1/1/6 {
 flexible-vlan-tagging;
 mtu 9192;
 encapsulation flexible-ethernet-services;
 unit 0 {
 encapsulation vlan-bridge;
 vlan-id 400;
 }
}
ge-1/1/5 {
 flexible-vlan-tagging;
 mtu 9192;
 encapsulation flexible-ethernet-services;
 unit 0 {
 encapsulation vlan-bridge;
 vlan-id 400;
 }
}
}
[edit bridge-domains]
bd1 {
 vlan-id 500;
 interface ge-1/1/6.0;
 interface ge-1/1/5.0;
}

[edit services rpm]
rfc2544-benchmarking {
 # Note, When in reflector mode, test profile is not needed
 tests {
 test-name l2b-reflector {
 interface ge-1/1/5.0;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 }
 family bridge;
 mode reflect;
 service-type elan;
 family bridge;
 direction egress;
 }
}
```

## Verifying the Results of the Benchmarking Tests for Layer 2 Services (E-LAN) in Bridge Domains

Examine the results of the benchmarking tests that are performed on the configured service between the ACX Router and the MX104 Router. Start the test on the reflector first and then start the test on the initiator.

- [Verifying the Throughput Benchmarking Test Results on page 278](#)
- [Verifying the Back-to-Back Benchmarking Test Results on page 280](#)

- [Verifying the Frame Loss Benchmarking Test Results on page 282](#)
- [Verifying the Latency Benchmarking Test Results on page 284](#)

### Verifying the Throughput Benchmarking Test Results

**Purpose** Verify that the necessary and statistical values are displayed for the benchmarking tests that are run on the configured service between the ACX router and the MX104 router.

**Action** In operational mode, enter the **show services rpm rfc2544-benchmarking test-id test-id-number detail** command on the ACX router.

```
user@host> show services rpm rfc2544-benchmarking test-id 1 detail
Test information :
 Test id: 1, Test name: tput_test, Test type: Throughput
 Test mode: Initiate-and-Terminate
 Test packet size: 128
 Test state: TEST_STATE_COMPLETED
 Status: Test-Completed
 Test start time: 2014-09-24 22:21:09 PDT
 Test finish time: 2014-09-24 22:21:33 PDT
 Counters last cleared: Never

 Test-profile Configuration:
 Test-profile name: tput
 Test packet size: 128
 Theoretical max bandwidth : 900000 kbps

 Test Configuration:
 Test mode: Initiate-and-Terminate
 Duration in seconds: 20
 Test finish wait duration in seconds: 1
 Test family: Bridge
 Test iterator pass threshold: 0.50 %
 Test receive failure threshold: 0.00 %
 Test transmit failure threshold: 0.50 %

 Bridge family Configuration:
 Interface : ge-1/1/3.0
 Test direction: Egress
 Source mac address: 00:00:00:00:11:11
 Destination mac address: 00:00:00:00:22:22
 Outer vlan-id: 400
 Outer vlan priority: 0
 Outer vlan cfi: 0
 Outer tag protocol id: 0x8100
 Source ipv4 address: 192.168.1.10
 Destination ipv4 address: 192.168.1.20
 Source udp port: 200
 Destination udp port: 200

 Rfc2544 throughput test information :
 Initial test load percentage : 100.00 %
 Test iteration mode : Binary
 Test iteration step : 50.00 %
 Theoretical max bandwidth : 900000 kbps
```

Test packet size: 128

| Iteration | Internal Overhead | Duration (sec) | Elapsed time | -----<br>Theoretical | Throughput<br>Transmit | -----<br>Measured |
|-----------|-------------------|----------------|--------------|----------------------|------------------------|-------------------|
|-----------|-------------------|----------------|--------------|----------------------|------------------------|-------------------|



```
1 0 20 20 100.00 % 100.00 % 100.00 %
```

Result of the iteration runs : Throughput Test complete for packet size 128  
 Best iteration : 1, Best iteration (pps) : 760135  
 Best iteration throughput : 100.00 %

RFC2544 Throughput test results summary:

```

Packet Internal Theoretical Transmit Tx Rx Measured
Size Measured
bandwidth overhead rate (pps) pps Packets Packets throughput %
(kbps)
128 0 760135 760135 15202700 15202700 100.00 %
900000
```

In operational mode, enter the **show services rpm rfc2544-benchmarking test-id test-id-number detail** command on the MX104 router.

```
user@host> show services rpm rfc2544-benchmarking test-id 1 detail
Test information :
 Test id: 1, Test name: 12b-reflector, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: TEST_STATE_RUNNING
 Status: Running
 Test start time: 2014-09-24 22:20:54 PDT
 Test finish time: TEST_RUNNING
 Counters last cleared: Never

Test Configuration:
 Test mode: Reflect
 Duration in seconds: 864000
 Test finish wait duration in seconds: 1
 Test family: Bridge
 Test iterator pass threshold: 0.50 %
 Test receive failure threshold: 0.00 %
 Test transmit failure threshold: 0.50 %

Bridge family Configuration:
 Interface : ge-1/1/5.0
 Test direction: Egress
 Source mac address: 00:00:00:00:11:11
 Destination mac address: 00:00:00:00:22:22
 Service type: Elan
```

```
Elapsed Reflected Reflected
time Packets Bytes
61 15202700 1945945600
```

You can also use the **show services rpm rfc2544-benchmarking (aborted-test | active-tests | completed-tests | summary)** command to display information about the results of each category or state of the RFC2544-based benchmarking 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 **run show services rpm rfc2544-benchmarking** operational command, see **show services rpm rfc2544-benchmarking** in the CLI Explorer.

### Verifying the Back-to-Back Benchmarking Test Results

**Purpose** Verify that the necessary and statistical values are displayed for the benchmarking tests that are run on the configured service between the ACX router and the MX104 router.

**Action** In operational mode, enter the **show services rpm rfc2544-benchmarking test-id test-id-number detail** command on the ACX router.

```
user@host> show services rpm rfc2544-benchmarking test-id 4 detail
Test information :
 Test id: 4, Test name: b2b-test, Test type: Back-Back-Frames
 Test mode: Initiate-and-Terminate
 Test packet size: 128 512
 Test state: TEST_STATE_COMPLETED
 Status: Test-Completed
 Test start time: 2014-09-24 22:30:16 PDT
 Test finish time: 2014-09-24 22:31:03 PDT
 Counters last cleared: Never

 Test-profile Configuration:
 Test-profile name: b2bt
 Test packet size: 128 512
 Theoretical max bandwidth : 950000 kbps

 Test Configuration:
 Test mode: Initiate-and-Terminate
 Duration in seconds: 20
 Test finish wait duration in seconds: 1
 Test family: Bridge
 Test iterator pass threshold: 0.50 %
 Test receive failure threshold: 0.00 %
 Test transmit failure threshold: 0.50 %

 Bridge family Configuration:
 Interface : ge-1/1/3.0
 Test direction: Egress
 Source mac address: 00:00:00:00:11:11
 Destination mac address: 00:00:00:00:22:22
 Outer vlan-id: 400
 Outer vlan priority: 0
 Outer vlan cfi: 0
 Outer tag protocol id: 0x8100
 Source ipv4 address: 192.168.1.10
 Destination ipv4 address: 192.168.1.20
 Source udp port: 4040
 Destination udp port: 4041

 Rfc2544 Back-Back test information :
 Initial burst length: 20 seconds at 950000 kbps
 Test iteration mode : Binary
 Test iteration step : 50.00 %
```

```
Test packet size: 128
Iteration Theoretical Transmit Internal Duration Elapsed
 burst length burst length overhead time
 (packets) (packets)
1 16047280 16047280 0 20 20
```

Result of the iteration runs : Back-Back Test complete for packet size 128

```

Best iteration : 1
Measured burst (num sec) : 20 sec
Measured burst (num pkts) : 16047280 packets

```

```

Test packet size: 512
Iteration Theoretical Transmit Internal Duration Elapsed
 burst length burst length overhead time
 (packets) (packets)
1 4464280 4464280 0 20 20

```

Result of the iteration runs : Back-Back Test complete for packet size 512

```

Best iteration : 1
Measured burst (num sec) : 20 sec
Measured burst (num pkts) : 4464280 packets

```

RFC2544 Back-Back test results summary:

```

Packet Measured Burst Time
Size length (Packets) (seconds)
128 16047280 20
512 4464280 20

```

In operational mode, enter the **show services rpm rfc2544-benchmarking test-id test-id-number detail** command on the MX104 router.

```

user@host> show services rpm rfc2544-benchmarking test-id 4 detail
Test information :
 Test id: 4, Test name: l2b-reflector, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: TEST_STATE_RUNNING
 Status: Running
 Test start time: 2014-09-24 22:30:07 PDT
 Test finish time: TEST_RUNNING
 Counters last cleared: Never

```

```

Test Configuration:
 Test mode: Reflect
 Duration in seconds: 864000
 Test finish wait duration in seconds: 1
 Test family: Bridge
 Test iterator pass threshold: 0.50 %
 Test receive failure threshold: 0.00 %
 Test transmit failure threshold: 0.50 %

```

```

Bridge family Configuration:
 Interface : ge-1/1/5.0
 Test direction: Egress
 Source mac address: 00:00:00:00:11:11
 Destination mac address: 00:00:00:00:22:22
 Service type: Elan

```

```

Elapsed Reflected Reflected
time Packets Bytes
58 20511560 4339763200

```

You can also use the **show services rpm rfc2544-benchmarking (aborted-test | active-tests | completed-tests | summary)** command to display information about the results of each

category or state of the RFC2544-based benchmarking 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 **run show services rpm rfc2544-benchmarking** operational command, see **show services rpm rfc2544-benchmarking** in the CLI Explorer.

### Verifying the Frame Loss Benchmarking Test Results

**Purpose** Verify that the necessary and statistical values are displayed for the benchmarking tests that are run on the configured service between the ACX router and the MX104 router.

**Action** In operational mode, enter the **show services rpm rfc2544-benchmarking test-id test-id-number detail** command on the ACX router.

```
user@host> show services rpm rfc2544-benchmarking test-id 3 detail
Test information :
 Test id: 3, Test name: frloss-test, Test type: Frame-Loss
 Test mode: Initiate-and-Terminate
 Test packet size: 1600
 Test state: TEST_STATE_COMPLETED
 Status: Test-Completed
 Test start time: 2014-09-24 22:26:45 PDT
 Test finish time: 2014-09-24 22:27:55 PDT
 Counters last cleared: Never

Test-profile Configuration:
 Test-profile name: frloss
 Test packet size: 1600
 Theoretical max bandwidth : 1000000 kbps

Test Configuration:
 Test mode: Initiate-and-Terminate
 Duration in seconds: 20
 Test finish wait duration in seconds: 1
 Test family: Bridge
 Test iterator pass threshold: 0.50 %
 Test receive failure threshold: 0.00 %
 Test transmit failure threshold: 0.50 %

Bridge family Configuration:
 Interface : ge-1/1/3.0
 Test direction: Egress
 Source mac address: 00:00:00:00:11:11
 Destination mac address: 00:00:00:00:22:22
 Outer vlan-id: 400
 Outer vlan priority: 0
 Outer vlan cfi: 0
 Outer tag protocol id: 0x8100
 Source ipv4 address: 192.168.1.10
 Destination ipv4 address: 192.168.1.20
 Source udp port: 200
 Destination udp port: 200

Rfc2544 frame-loss test information :
 Initial test load percentage : 100.00 %
 Test iteration mode : step-down
 Test iteration step : 10 %
```

Theoretical max bandwidth : 1000000 kbps

Test packet size: 1600

Iteration Internal Duration Elapsed ----- Throughput ----- Frame-loss

|   | Overhead | (sec) | time | Theoretical | Transmit Measured | rate %          |
|---|----------|-------|------|-------------|-------------------|-----------------|
| 1 | 0        | 20    | 20   | 100.00 %    | 100.00 %          | 100.00 % 0.00 % |
| 2 | 0        | 20    | 20   | 100.00 %    | 100.00 %          | 100.00 % 0.00 % |
| 3 | 0        | 20    | 20   | 100.00 %    | 100.00 %          | 100.00 % 0.00 % |

Result of the iteration runs : Frame-loss test complete for packet size 1600

Percentage throughput transmitted: 100.00 %

Frame-loss rate (percent) : 0.00 %

RFC2544 Frame-loss test results summary:

| Packet<br>Size | Internal<br>Frame Loss<br>overhead<br>rate percent | Theoretical<br>rate (pps) | Transmit<br>pps | Transmit<br>throughput | Tx<br>Packets | Rx<br>Packets |
|----------------|----------------------------------------------------|---------------------------|-----------------|------------------------|---------------|---------------|
| 1600           | 0                                                  | 77160                     | 77160           | 100.00 %               | 1543200       | 1543200       |
|                | 0.00 %                                             |                           |                 |                        |               |               |

In operational mode, enter the **show services rpm rfc2544-benchmarking test-id test-id-number detail** command on the MX104 router.

user@host> **show services rpm rfc2544-benchmarking test-id 3 detail**

Test information :

Test id: 3, Test name: l2b-reflector, Test type: Reflect  
 Test mode: Reflect  
 Test packet size: 0  
 Test state: TEST\_STATE\_RUNNING  
 Status: Running  
 Test start time: 2014-09-24 22:25:36 PDT  
 Test finish time: TEST\_RUNNING  
 Counters last cleared: Never

Test Configuration:

Test mode: Reflect  
 Duration in seconds: 864000  
 Test finish wait duration in seconds: 1  
 Test family: Bridge  
 Test iterator pass threshold: 0.50 %  
 Test receive failure threshold: 0.00 %  
 Test transmit failure threshold: 0.50 %

Bridge family Configuration:

Interface : ge-1/1/5.0  
 Test direction: Egress  
 Source mac address: 00:00:00:00:11:11  
 Destination mac address: 00:00:00:00:22:22  
 Service type: Elan

| Elapsed<br>time | Reflected<br>Packets | Reflected<br>Bytes |
|-----------------|----------------------|--------------------|
| 95              | 1624361              | 2598977600         |

You can also use the **show services rpm rfc2544-benchmarking (aborted-test | active-tests | completed-tests | summary)** command to display information about the results of each

category or state of the RFC2544-based benchmarking 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 **run show services rpm rfc2544-benchmarking** operational command, see **show services rpm rfc2544-benchmarking** in the CLI Explorer.

---

### Verifying the Latency Benchmarking Test Results

---

**Purpose** Verify that the necessary and statistical values are displayed for the benchmarking tests that are run on the configured service between the ACX router and the MX104 router.

**Action** In operational mode, enter the **show services rpm rfc2544-benchmarking test-id test-id-number detail** command on the ACX router.

```
user@host> show services rpm rfc2544-benchmarking test-id 5 detail
```

```
Test information :
```

```
Test id: 5, Test name: lty-test, Test type: Latency
Test mode: Initiate-and-Terminate
Test packet size: 512
Test state: TEST_STATE_COMPLETED
Status: Test-Completed
Test start time: 2014-09-24 22:33:05 PDT
Test finish time: 2014-09-24 22:40:46 PDT
Counters last cleared: Never
```

```
Test-profile Configuration:
```

```
Test-profile name: lty
Test packet size: 512
Theoretical max bandwidth : 1000000 kbps
```

```
Test Configuration:
```

```
Test mode: Initiate-and-Terminate
Duration in seconds: 20
Test finish wait duration in seconds: 1
Test family: Bridge
Test iterator pass threshold: 0.50 %
Test receive failure threshold: 0.00 %
Test transmit failure threshold: 0.50 %
```

```
Bridge family Configuration:
```

```
Interface : ge-1/1/3.0
Test direction: Egress
Source mac address: 00:00:00:00:11:11
Destination mac address: 00:00:00:00:22:22
Outer vlan-id: 400
Outer vlan priority: 0
Outer vlan cfi: 0
Outer tag protocol id: 0x8100
Source ipv4 address: 192.168.1.10
Destination ipv4 address: 192.168.1.20
Source udp port: 200
Destination udp port: 200
```

```
Rfc2544 latency test information :
```

```
Theoretical max bandwidth : 1000000 kbps
Initial test load percentage : 100.00 %
Duration in seconds: 20
```

Measurement unit for timestamp: Nanoseconds

Test packet size: 512

| Iteration | Duration | Elapsed | Theoretical | Transmit | Throughput |         |
|-----------|----------|---------|-------------|----------|------------|---------|
|           |          | Latency |             |          |            |         |
|           | (sec)    | time    | rate (pps)  | pps      | percent    | Minimum |
|           | Average  | Maximum | Probe       |          |            |         |
| 1         | 20       | 20      | 234962      | 234962   | 100.00 %   | 44008   |
|           | 45253    | 47424   | 45096       |          |            |         |
| 2         | 20       | 20      | 234962      | 234962   | 100.00 %   | 44008   |
|           | 45237    | 47456   | 45256       |          |            |         |
| 3         | 20       | 20      | 234962      | 234962   | 100.00 %   | 43864   |
|           | 45198    | 46976   | 45144       |          |            |         |
| 4         | 20       | 20      | 234962      | 234962   | 100.00 %   | 43832   |
|           | 45243    | 47088   | 45096       |          |            |         |
| 5         | 20       | 20      | 234962      | 234962   | 100.00 %   | 44072   |
|           | 45261    | 46976   | 45176       |          |            |         |
| 6         | 20       | 20      | 234962      | 234962   | 100.00 %   | 43784   |
|           | 45214    | 46864   | 45032       |          |            |         |
| 7         | 20       | 20      | 234962      | 234962   | 100.00 %   | 44024   |
|           | 45259    | 47216   | 45240       |          |            |         |
| 8         | 20       | 20      | 234962      | 234962   | 100.00 %   | 44072   |
|           | 45290    | 46864   | 45192       |          |            |         |
| 9         | 20       | 20      | 234962      | 234962   | 100.00 %   | 43976   |
|           | 45272    | 46792   | 45208       |          |            |         |
| 10        | 20       | 20      | 234962      | 234962   | 100.00 %   | 44024   |
|           | 45206    | 46976   | 45112       |          |            |         |
| 11        | 20       | 20      | 234962      | 234962   | 100.00 %   | 44040   |
|           | 45198    | 47088   | 45176       |          |            |         |
| 12        | 20       | 20      | 234962      | 234962   | 100.00 %   | 44008   |
|           | 45223    | 46976   | 45160       |          |            |         |
| 13        | 20       | 20      | 234962      | 234962   | 100.00 %   | 44088   |
|           | 45257    | 47408   | 45176       |          |            |         |
| 14        | 20       | 20      | 234962      | 234962   | 100.00 %   | 43976   |
|           | 45183    | 46832   | 45080       |          |            |         |
| 15        | 20       | 20      | 234962      | 234962   | 100.00 %   | 44024   |
|           | 45198    | 47088   | 45112       |          |            |         |
| 16        | 20       | 20      | 234962      | 234962   | 100.00 %   | 43864   |
|           | 45206    | 46912   | 45208       |          |            |         |
| 17        | 20       | 20      | 234962      | 234962   | 100.00 %   | 44056   |
|           | 45209    | 46960   | 45176       |          |            |         |
| 18        | 20       | 20      | 234962      | 234962   | 100.00 %   | 44008   |
|           | 45198    | 46912   | 45112       |          |            |         |
| 19        | 20       | 20      | 234962      | 234962   | 100.00 %   | 43816   |
|           | 45175    | 47248   | 45000       |          |            |         |
| 20        | 20       | 20      | 234962      | 234962   | 100.00 %   | 43912   |
|           | 45202    | 46992   | 45192       |          |            |         |

Result of the iteration runs : Latency Test complete for packet size 512

Internal overhead per packet: 0

Avg (min) Latency : 43972

Avg (avg) latency : 45224

Avg (Max) latency : 47052

Avg (probe) latency : 45147

RFC2544 Latency test results summary:

| Packet | Internal | Theoretical | Transmit | Tx      | Rx      |         |
|--------|----------|-------------|----------|---------|---------|---------|
| Size   | overhead | Latency     |          |         |         | Minimum |
|        |          | rate (pps)  | pps      | Packets | Packets |         |

|         |         |        |        |          |          |
|---------|---------|--------|--------|----------|----------|
| Average | Maximum | Probe  |        |          |          |
| 512     | 0       | 234962 | 234962 | 93984800 | 93984800 |
| 45224   | 47052   | 45147  |        |          | 43972    |

In operational mode, enter the **show services rpm rfc2544-benchmarking test-id test-id-number detail** command on the MX104 router.

```
user@host> show services rpm rfc2544-benchmarking test-id 5 detail
Test information :
 Test id: 5, Test name: 12b-reflector, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: TEST_STATE_RUNNING
 Status: Running
 Test start time: 2014-09-24 22:32:55 PDT
 Test finish time: TEST_RUNNING
 Counters last cleared: Never

 Test Configuration:
 Test mode: Reflect
 Duration in seconds: 864000
 Test finish wait duration in seconds: 1
 Test family: Bridge
 Test iterator pass threshold: 0.50 %
 Test receive failure threshold: 0.00 %
 Test transmit failure threshold: 0.50 %

 Bridge family Configuration:
 Interface : ge-1/1/5.0
 Test direction: Egress
 Source mac address: 00:00:00:00:11:11
 Destination mac address: 00:00:00:00:22:22
 Service type: Elan
```

|         |           |             |
|---------|-----------|-------------|
| Elapsed | Reflected | Reflected   |
| time    | Packets   | Bytes       |
| 426     | 84586320  | 43308195840 |

You can also use the **show services rpm rfc2544-benchmarking (aborted-test | active-tests | completed-tests | summary)** command to display information about the results of each category or state of the RFC2544-based benchmarking 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 **run show services rpm rfc2544-benchmarking** operational command, see **show services rpm rfc2544-benchmarking** in the CLI Explorer.

**Related Documentation**

- [RFC2544-Based Benchmarking Tests for E-LAN and E-Line Services Overview on page 231](#)
- [Supported RFC2544-Based Benchmarking Statements on MX104 Routers on page 234](#)



## Example: Configuring Benchmarking Tests to Measure SLA Parameters for E-LAN Services Using VPLS

---

This example shows how to configure benchmarking tests for the E-LAN services using BGP-based VPLS. The example covers the four benchmarking tests: throughput, frame loss, back-to-back frames, and latency.

- [Requirements on page 287](#)
- [Overview on page 287](#)
- [Configuration on page 288](#)
- [Verifying the Results of the Benchmarking Test for Layer 2 ELAN Services Using VPLS on page 307](#)

### Requirements

This example uses the following hardware and software components:

- An MX104 3D Universal Edge router
- Any MX Series router
- Any ACX Series router
- Junos OS Release 15.1 or later for MX Series routers

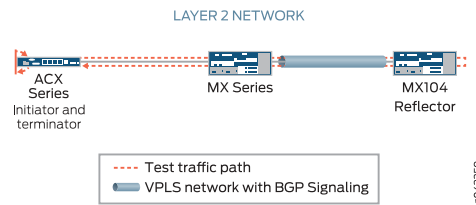
### Overview

Consider a sample topology in which an ACX Series router functions as an initiator and terminator of the test frames for an RFC2544-based benchmarking test. The ACX Series router is connected to a provider edge router, PE1 (an MX Series router). The PE1 router is configured with a VPLS routing instance and is connected over a Layer 2 network to another provider edge router, PE2 (an MX104 router). A simple VPLS network with BGP signalling is created between routers PE1 and PE2. The MX104 router also functions as a reflector to reflect the test frames it receives from the ACX Series router back to the initiator.

Benchmarking tests compute the performance attributes in the user-to-network interface (UNI) direction of the Layer 2 E-LAN service between the ACX Series router and the MX104 router. To measure SLA parameters for E-LAN services using VPLS, configure specific benchmarking tests. In this example, all four benchmarking tests (throughput, back-to-back frames, latency, and frame-loss) are configured.

[Figure 13 on page 288](#) shows the sample topology to perform all four RFC2544-based benchmarking tests for the UNI direction on a Layer 2 network using VPLS.

Figure 13: Layer 2 Reflection with Simple BGP-based VPLS Topology



On the ACX Series router, ge-0/2/1.0 is the Layer 2 NNI interface and ge-0/2/0.0 is the Layer 2 UNI interface. For each benchmarking test configured on the ACX Series router, specify the source MAC address as 00:00:00:00:11:11 and 00:00:00:00:22:22 as the destination MAC address. Also, specify the VLAN ID as 512. On the MX Series router, ge-0/3/0.0 is the Layer 2 NNI interface and ge-0/2/1.0 is the UNI interface. On the MX104 router, ge-0/2/5.0 is the Layer 2 NNI interface and ge-0/3/1.0 is the Layer 2 UNI interface. The benchmarking tests are used to compute the performance attributes for an E-LAN service using VPLS.

## Configuration

In this example, you configure the benchmarking tests for the UNI direction for a Layer 2 E-LAN service using VPLS between two routers (initiator and reflector) to detect and analyze the performance of the interconnected routers. The initiator and reflector routers are not directly connected to each other. The initiator is connected to a provider edge router (PE1), which is in turn connected to the reflector. In this example, the ACX Series router is the initiator, an MX Series router is PE1, and the MX104 router is the other provider edge router (PE2) and reflector. Start by configuring the initiator. On the ACX Series router, you first configure each test by specifying the test profile and the test attributes, and then define the test by associating the test with the test profile with the relevant attributes. You can then configure the interface. On the MX Series router, configure the VPLS parameters to enable VPLS on the router. On the MX104 router, configure the benchmarking parameters and the VPLS parameters.



**NOTE:** When you configure Layer 2 reflection, you can specify the service type under test as ELINE if you want to simulate an ELINE service that by using bridge encapsulation.

- [Configuring Throughput Benchmarking Test Parameters on the ACX Series Router \(Initiator\) on page 293](#)
- [Configuring Back-to-Back Frames Benchmarking Test Parameters on the ACX Series Router on page 294](#)
- [Configuring Latency Benchmarking Test Parameters on the ACX Series Router on page 295](#)
- [Configuring Frame Loss Benchmarking Test Parameters on the ACX Series Router on page 297](#)
- [Configuring Other Benchmarking Test Parameters on the ACX Series Router on page 298](#)

- [Configuring the VPLS Parameters on the MX Series Router \(PE1\) on page 299](#)
- [Configuring Benchmarking Test Parameters on the MX104 Router \(Reflector\) on page 300](#)
- [Configuring Other Benchmarking Test Parameters on the MX104 Router \(Reflector\) on page 301](#)
- [Configuring VPLS Parameters on the MX104 Router \(Reflector\) on page 302](#)
- [Results on page 303](#)

#### 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 the ACX Series Router (Initiator)

```
set services rpm rfc2544-benchmarking profiles test-profile tput test-type throughput
set services rpm rfc2544-benchmarking profiles test-profile tput packet-size 256
set services rpm rfc2544-benchmarking profiles test-profile tput bandwidth-kbps 600000
set services rpm rfc2544-benchmarking profiles test-profile b2bt test-type
 back-back-frames
set services rpm rfc2544-benchmarking profiles test-profile b2bt packet-size 9104
set services rpm rfc2544-benchmarking profiles test-profile b2bt bandwidth-kbps 600000
set services rpm rfc2544-benchmarking profiles test-profile lty test-type latency
set services rpm rfc2544-benchmarking profiles test-profile lty packet-size 1024
set services rpm rfc2544-benchmarking profiles test-profile lty bandwidth-kbps 6000000
set services rpm rfc2544-benchmarking profiles test-profile frloss test-type frame-loss
set services rpm rfc2544-benchmarking profiles test-profile frloss packet-size 1600
set services rpm rfc2544-benchmarking profiles test-profile frloss bandwidth-kbps
 6000000
set services rpm rfc2544-benchmarking profiles test-profile frloss step-percent 5
set services rpm rfc2544-benchmarking tests test-name tput-test test-profile tput
set services rpm rfc2544-benchmarking tests test-name tput-test source-mac-address
 00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name tput-test destination-mac-address
 00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name tput-test ovlan-id 512
set services rpm rfc2544-benchmarking tests test-name tput-test service-type elan
set services rpm rfc2544-benchmarking tests test-name tput-test mode
 initiate-and-terminate
set services rpm rfc2544-benchmarking tests test-name tput-test family bridge
set services rpm rfc2544-benchmarking tests test-name tput-test direction egress
set services rpm rfc2544-benchmarking tests test-name tput-test source-udp-port 200
set services rpm rfc2544-benchmarking tests test-name tput-test destination-udp-port
 400
set services rpm rfc2544-benchmarking tests test-name tput-test test-iterator-duration
 250
set services rpm rfc2544-benchmarking tests test-name tput-test test-interface ge-0/2/0.0
set services rpm rfc2544-benchmarking tests test-name b2bt-test test-profile b2bt
set services rpm rfc2544-benchmarking tests test-name b2bt-test source-mac-address
 00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name b2bt-test destination-mac-address
 00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name b2bt-test ovlan-id 512
set services rpm rfc2544-benchmarking tests test-name b2bt-test service-type elan
set services rpm rfc2544-benchmarking tests test-name b2bt-test mode
 initiate-and-terminate
set services rpm rfc2544-benchmarking tests test-name b2bt-test family bridge
```

```
set services rpm rfc2544-benchmarking tests test-name b2bt-test direction egress
set services rpm rfc2544-benchmarking tests test-name b2bt--test destination-udp-port
 400
set services rpm rfc2544-benchmarking tests test-name b2bt-test test-iterator-duration
 10
set services rpm rfc2544-benchmarking tests test-name b2b-test test-interface ge-0/2/0.0
set services rpm rfc2544-benchmarking tests test-name lty-test test-profile lty
set services rpm rfc2544-benchmarking tests test-name lty-test source-mac-address
 00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name lty-test destination-mac-address
 00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name lty-test ovlan-id 512
set services rpm rfc2544-benchmarking tests test-name lty-test service-type elan
set services rpm rfc2544-benchmarking tests test-name lty-test mode
 initiate-and-terminate
set services rpm rfc2544-benchmarking tests test-name lty-test family bridge
set services rpm rfc2544-benchmarking tests test-name lty-test direction egress
set services rpm rfc2544-benchmarking tests test-name lty-test source-udp-port 200
set services rpm rfc2544-benchmarking tests test-name lty-test destination-udp-port
 400
set services rpm rfc2544-benchmarking tests test-name lty-test test-iterator-duration 10
set services rpm rfc2544-benchmarking tests test-name lty-test test-interface ge-0/2/0.0
set services rpm rfc2544-benchmarking tests test-name frloss-test test-profile frloss
set services rpm rfc2544-benchmarking tests test-name frloss-test source-mac-address
 00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name frloss-test
 destination-mac-address 00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name frloss-test ovlan-id 512
set services rpm rfc2544-benchmarking tests test-name frloss-test ovlan-priority 7
set services rpm rfc2544-benchmarking tests test-name frloss-test ovlan-cfi 1
set services rpm rfc2544-benchmarking tests test-name frloss-test service-type elan
set services rpm rfc2544-benchmarking tests test-name frloss-test mode
 initiate-and-terminate
set services rpm rfc2544-benchmarking tests test-name frloss-test family bridge
set services rpm rfc2544-benchmarking tests test-name frloss-test direction egress
set services rpm rfc2544-benchmarking tests test-name frloss-test source-udp-port 200
set services rpm rfc2544-benchmarking tests test-name frloss-test destination-udp-port
 400
set services rpm rfc2544-benchmarking tests test-name frloss-test test-iterator-duration
 30
set services rpm rfc2544-benchmarking tests test-name frloss-test test-interface
 ge-0/2/0.0
set interfaces ge-0/2/0 flexible-vlan-tagging
set interfaces ge-0/2/0 mtu 9192
set interfaces ge-0/2/0 encapsulation flexible-ethernet-services
set interfaces ge-0/2/0 unit 0 encapsulation vlan-bridge
set interfaces ge-0/2/0 unit 0 vlan-id 512
set interfaces ge-0/2/1 flexible-vlan-tagging
set interfaces ge-0/2/1 mtu 9192
set interfaces ge-0/2/1 encapsulation flexible-ethernet-services
set interfaces ge-0/2/1 unit 0 encapsulation vlan-bridge
set interfaces ge-0/2/1 unit 0 vlan-id 512
set bridge-domains bd1 vlan-id 10
set bridge-domains bd1 interface ge-0/2/1.0
set bridge-domains bd1 interface ge-0/2/0.0
```

**Configuring VPLS  
Parameters on the MX  
Router (Provider Edge  
Router PE1)**

```
set chassis fpc 0 pic 2 tunnel-services
set interfaces ge-0/2/1 flexible-vlan-tagging
set interfaces ge-0/2/1 mtu 9192
set interfaces ge-0/2/1 encapsulation vlan-vpls
set interfaces ge-0/2/1 unit 0 encapsulation vlan-vpls
set interfaces ge-0/2/1 unit 0 vlan-id 512
set interfaces ge-0/3/0 mtu 9192
set interfaces ge-0/3/0 unit 0 family inet address 32.0.0.1/24
set interfaces ge-0/3/0 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 100.1.1.1/32
set routing-options router-id 100.1.1.1
set routing-options autonomous-system 100
set protocols mpls interface ge-0/3/0.0
set protocols bgp group test type internal
set protocols bgp group test local-address 100.1.1.1
set protocols bgp group test family l2vpn signaling
set protocols bgp group test neighbor 100.1.1.2
set protocols ospf traffic-engineering
set protocols ospf reference-bandwidth 1g
set protocols ospf area 0.0.0.0 interface ge-0/3/0.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ldp interface ge-0/3/0.0 set protocols ldp interface lo0.0
set routing-instances vpls-pe1 instance-type vpls
set routing-instances vpls-pe1 interface ge-0/2/1.0
set routing-instances vpls-pe1 no-local-switching
set routing-instances vpls-pe1 route-distinguisher 100.1.1.1:101
set routing-instances vpls-pe1 vrf-target target:1:2
set routing-instances vpls-pe1 protocols vpls site-range 8
set routing-instances vpls-pe1 protocols vpls no-tunnel-services
set routing-instances vpls-pe1 protocols vpls site HUB site-identifier 1
set routing-instances vpls-pe1 protocols vpls vpls-id 1
set routing-instances vpls-pe1 protocols vpls neighbor 100.1.1.2
```

**Configuring  
Benchmarking Test  
Parameters and VPLS  
Parameters on the  
MX104 Router  
(Provider Edge Router  
PE2)**

```
set services rpm rfc2544-benchmarking tests test-name l2v-reflector source-mac-address
00:00:00:00:11:11
set services rpm rfc2544-benchmarking tests test-name l2v-reflector
destination-mac-address 00:00:00:00:22:22
set services rpm rfc2544-benchmarking tests test-name l2v-reflector service-type elan
set services rpm rfc2544-benchmarking tests test-name l2v-reflector in-service
set services rpm rfc2544-benchmarking tests test-name l2v-reflector ip-swap
set services rpm rfc2544-benchmarking tests test-name l2v-reflector udp-tcp-port-swap
set services rpm rfc2544-benchmarking tests test-name l2v-reflector mode reflect
set services rpm rfc2544-benchmarking tests test-name l2v-reflector family vpls
set services rpm rfc2544-benchmarking tests test-name l2v-reflector reflect-etype 2048
set services rpm rfc2544-benchmarking tests test-name l2v-reflector direction egress
set services rpm rfc2544-benchmarking tests test-name l2v-reflector source-udp-port
200
set services rpm rfc2544-benchmarking tests test-name l2v-reflector destination-udp-port
200
set services rpm rfc2544-benchmarking tests test-name l2v-reflector test-interface
ge-0/3/1.0
set interfaces ge-0/2/5 mtu 9192
set interfaces ge-0/2/5 unit 0 family inet address 42.0.0.1/24
set interfaces ge-0/2/5 unit 0 family mpls
set interfaces ge-0/3/1 flexible-vlan-tagging
```

```
set interfaces ge-0/3/1 mtu 9192
set interfaces ge-0/3/1 encapsulation vlan-vpls
set interfaces ge-0/3/1 unit 0 encapsulation vlan-vpls
set interfaces ge-0/3/1 unit 0 vlan-id 512
set interfaces ge-0/3/1 unit 0 family vpls filter input portmirror
set interfaces ge-0/3/1 unit 0 family vpls filter output portmirror
set interfaces ge-0/3/2 flexible-vlan-tagging
set interfaces ge-0/3/2 mtu 9192
set interfaces ge-0/3/2 encapsulation vlan-vpls
set interfaces ge-0/3/2 unit 0 encapsulation vlan-vpls
set interfaces ge-0/3/2 unit 0 vlan-id 512
set interfaces lo0 unit 0 family inet address 100.1.1.2/32
set forwarding-options port-mirroring input rate 1
set forwarding-options port-mirroring family vpls output interface ge-0/3/3.0
set forwarding-options port-mirroring family vpls output no-filter-check
set forwarding-options port-mirroring instance pm1 input rate 10000
set forwarding-options port-mirroring instance pm1 family vpls output interface ge-0/3/3.0
set routing-options router-id 100.1.1.2
set routing-options autonomous-system 100
set protocols mpls interface ge-0/2/5.0
set protocols bgp group test type internal
set protocols bgp group test local-address 100.1.1.2
set protocols bgp group test family l2vpn signaling
set protocols bgp group test neighbor 100.1.1.1
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface ge-0/2/5.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ldp interface ge-0/2/5.0
set protocols ldp interface lo0.0
set firewall family vpls filter portmirror term 1 then count pm1
set firewall family vpls filter portmirror term 1 then accept
set firewall family vpls filter portmirror term 1 then port-mirror
set routing-instances vpls-pe2 instance-type vpls
set routing-instances vpls-pe2 interface ge-0/3/1.0
set routing-instances vpls-pe2 interface ge-0/3/3.0
set routing-instances vpls-pe2 no-local-switching
set routing-instances vpls-pe2 route-distinguisher 100.1.1.2:102
set routing-instances vpls-pe2 vrf-target target:1:2
set routing-instances vpls-pe2 protocols vpls site-range 8
set routing-instances vpls-pe2 protocols vpls no-tunnel-services
set routing-instances vpls-pe2 protocols vpls site SPOKE site-identifier 2
set routing-instances vpls-pe2 protocols vpls vpls-id 1
set routing-instances vpls-pe2 protocols vpls neighbor 100.1.1.1
```

### Configuring Throughput Benchmarking Test Parameters on the ACX Series Router (Initiator)

#### Step-by-Step Procedure

The following configuration requires you to configure a test profile for the throughput test and reference the test profile in a unique test name. The test name defines the parameters for the throughput test to be performed on the ACX Series router.

To configure the throughput test parameters on the ACX Series router:

1. In configuration mode, at the `[edit]` hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```

2. Define a name for the first test profile—for example, `tput`—for the throughput test profile.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit profiles test-profile tput
```

3. Configure the type of test to be performed as throughput, specify the packet size as 256 bytes, and define the theoretical maximum bandwidth for the test as 600000 Kbps. You can specify any value from 1 Kbps through 1,000,000 Kbps for the maximum bandwidth.

```
[edit services rpm rfc2544-benchmarking profiles test-profile tput]
user@host# set test-type throughput packet-size 256 bandwidth-kbps 600000
```

4. Enter the `up` command twice to go to the `[edit services rpm rfc2544-benchmarking]` level in the configuration hierarchy.

```
[edit services rpm rfc2544-benchmarking profiles test-profile tput]
user@host# up
user@host# up
```

5. Define a name for the throughput test—for example, `tput-test`. The test name can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name tput-test
```

6. Specify the name of the test profile, `tput`, to be associated with the test name.

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set test-profile tput
```

7. Configure the source and destination MAC addresses for the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address
00:00:00:00:22:22
```

8. Configure the outer VLAN ID for the test frames and specify the service type under test to be E-LAN.

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set ovlan-id 512 service-type elan
```

9. 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 tput-test]
user@host# set mode initiate-and-terminate
```
10. Configure the family type, **bridge**, for the benchmarking test and specify the direction, egress. Also, specify the source and destination UDP ports to be used in the UDP headers of the test packet.  

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set family bridge direction egress source-udp-port 200
destination-udp-port 400
```
11. Specify the duration of each iteration in seconds, with a value from 10 seconds to 1,728,000 seconds, and specify the logical interface, `ge-0/2/0.0`, on which the RFC2544-benchmarking tests are run.  

```
[edit services rpm rfc2544-benchmarking tests test-name tput-test]
user@host# set test-iterator-duration 250 test-interface ge-0/2/0.0
```

---

### Configuring Back-to-Back Frames Benchmarking Test Parameters on the ACX Series Router

---

#### Step-by-Step Procedure

The following configuration requires you to configure a test profile for the back-to-back frames test and reference the test profile in a unique test name. The test name defines the parameters for the back-to-back frames test to be performed on the ACX Series router.

To configure the back-to-back frames test parameters on the ACX Series router:

1. In configuration mode, at the `[edit]` hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.  

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```
2. Define a name for the back-to-back test profile—for example, `b2bt`.  

```
[edit services rpm rfc2544-benchmarking]
user@host# edit profiles test-profile b2bt
```
3. Configure the type of test to be performed as back-to-back frames, specify the packet size as 9104 bytes, and specify the theoretical maximum bandwidth for the test as 600000 Kbps. You can specify any value from 1 Kbps through 1,000,000 Kbps as the maximum bandwidth.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile b2bt]
user@host# set test-type back-to-back-frames packet-size 9104 bandwidth-kbps 600000
```
4. Enter the `up` command twice to go to the `[edit services rpm rfc2544-benchmarking]` level in the configuration hierarchy.  

```
[edit services rpm rfc2544-benchmarking profiles test-profile b2bt]
user@host# up
user@host# up
```



5. Define a name for the back-to-back frames test—for example, b2bt-test. The test name can be up to 32 characters in length.  

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name b2bt-test
```
6. Specify the name of the test profile, b2bt, to be associated with the test name.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set test-profile b2bt
```
7. Configure the source and destination MAC addresses for the test packet.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address
00:00:00:00:22:22
```
8. Configure the outer VLAN ID for the test frames and specify the service type under test as E-LAN.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set ovlan-id 512 service-type elan
```
9. 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 b2bt-test]
user@host# set mode initiate-and-terminate
```
10. Configure the family type, **bridge**, for the benchmarking test and specify the direction, egress.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set family bridge direction egress
```
11. Specify the duration of each iteration in seconds, with a value from 10 seconds to 1,728,000 seconds. Also, specify the logical interface, ge-0/2/0.0, on which the RFC2544-based benchmarking test is run.  

```
[edit services rpm rfc2544-benchmarking tests test-name b2bt-test]
user@host# set test-iterator-duration 10 test-interface ge-0/2/0.0
```

### Configuring Latency Benchmarking Test Parameters on the ACX Series Router

#### Step-by-Step Procedure

The following configuration requires you to configure a test profile for the latency test and reference the test-profile in a unique test-name. The test-name defines the parameters for the latency test to be performed on the initiator (ACX Series router).

To configure the latency test parameters on the initiator:

1. In configuration mode, at the **[edit]** hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.  

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```
2. Define a name for the latency test profile—for example, lty.  

```
[edit services rpm rfc2544-benchmarking]
```

```
user@host# edit profiles test-profile lty
```

3. Configure the type of test to be performed as latency, specify the packet size of the test packet as 1024, and specify the maximum bandwidth for the test in Kbps, with a value from 1 Kbps through 1,000,000 Kbps.

```
[edit services rpm rfc2544-benchmarking profiles]
```

```
user@host# set test-profile lty test-type latency packet-size 1024 bandwidth-kbps 600000
```

4. Enter the **up** command twice to go to the previous level in the configuration hierarchy.

```
[edit services rpm rfc2544-benchmarking profiles test-profile lty]
```

```
user@host# up
```

```
user@host# up
```

5. Define a name for the latency test—for example, lty-test. The test name can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
```

```
user@host# edit tests test-name lty-test
```

6. Specify the name of the test profile, lty, to be associated with the test name.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set test-profile lty
```

7. Configure the source and destination MAC addresses for the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address 00:00:00:00:22:22
```

8. Configure the outer VLAN ID for the test frames and specify the service type under test.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set ovlan-id 512 service-type elan
```

9. 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 lty-test]
```

```
user@host# set mode initiate-and-terminate
```

10. Configure the family type, **bridge**, for the benchmarking test and specify the direction, egress. Also, specify the source and destination UDP port to be used in the UDP headers of the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set family bridge direction egress source-udp-port 200 destination-udp-port 400
```

11. Specify the duration of each iteration in seconds, with a value from 10 seconds to 1,728,000 seconds. Also, specify the logical interface, ge-0/2/0.0, on which the RFC2544-based benchmarking test is run.

```
[edit services rpm rfc2544-benchmarking tests test-name lty-test]
```

```
user@host# set test-iterator-duration 10 test-interface ge-0/2/0.0
```

### Configuring Frame Loss Benchmarking Test Parameters on the ACX Series Router

#### Step-by-Step Procedure

The following configuration requires you to configure a test profile for the frame loss test and reference the test-profile in a unique test-name. The test-name defines the parameters for the frame loss test to be performed on the ACX router.

To configure the frame loss test parameters on the ACX Router:

1. In configuration mode, at the **[edit]** hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```

2. Define a name for the frame loss test profile—for example, frloss.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit profiles test-profile frloss
```

3. Configure the type of test performed as frame loss, specify the packet size of the test packet, and define the 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]
user@host# set test-profile frloss test-type frame-loss packet-size 1600
bandwidth-kbps 600000
```

4. Enter the **up** command to go to the previous level in the configuration hierarchy.

```
[edit services rpm rfc2544-benchmarking profiles]
user@host# up
```

5. Define a name for the frame loss test—for example, frloss-test. The test name can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name frloss-test
```

6. Specify the name of the test profile, frloss, to be associated with the test name.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set test-profile frloss
```

7. Configure the source and destination MAC address for the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address
00:00:00:00:22:22
```

8. Configure the outer VLAN ID, priority, and the canonical format indicator (cfi) value for the test frames. Together, the four added bytes, priority (3 bits) and canonical format indicator (1 bit) form the VLAN tag. Also, specify the service type under test.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set ovlan-id 512 ovlan-priority 7 ovlan-cfi 1 service-type elan
```

9. 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 frloss-test]
user@host# set mode initiate-and-terminate
```

10. Configure the family type, **bridge**, for the benchmarking test and specify the direction, egress. Also, specify the source and destination UDP port to be used in the UDP headers of the test packet.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set family bridge direction egress source-udp-port 200
destination-udp-port 400
```

11. Specify the duration of each iteration in seconds, with a value from 10 seconds to 1,728,000 seconds. Also, specify the logical interface, ge-0/2/1.0, on which the RFC2544-based benchmarking test is run.

```
[edit services rpm rfc2544-benchmarking tests test-name frloss-test]
user@host# set test-iterator-duration 30 test-interface ge-0/2/0.0
```

12. Enter the **exit** command to go to the [edit] hierarchy level.

```
[edit services rpm rfc2544-benchmarking tests test-name test4]
user@host# exit
```

---

### Configuring Other Benchmarking Test Parameters on the ACX Series Router

---

#### 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.

To configure the interface and bridge domain on the ACX Router:

1. Configure the Layer 2 NNI interface on which the tests must be run from the **[edit]** hierarchy level.

```
[edit]
user@host# edit interfaces ge-0/2/1
```

2. Configure flexible VLAN tagging for the transmission of untagged frames or 802.1Q single-tagged and dual-tagged frames on the logical interface. You can also specify the maximum transmission unit (MTU) size for the interface and the encapsulation.

```
[edit interfaces ge-0/2/1]
user@host# set flexible-vlan-tagging mtu 9192 encapsulation
flexible-ethernet-services
```

3. Configure a logical unit for the interface, specify the encapsulation, and configure the VLAN ID on the logical interfaces.

```
[edit interfaces ge-0/2/1]
user@host# set unit 0 encapsulation vlan-bridge vlan-id 512
```

4. Configure the Layer 2 UNI interface.

```
[edit]
user@host# edit interfaces ge-0/2/0
```

5. Configure flexible VLAN tagging for transmission of non-tagged frames or 802.1Q single-tag and dual-tag frames on the logical interface. You can also specify the maximum transmission unit (MTU) size for the interface and the encapsulation.

```
[edit interfaces ge-0/2/0]
user@host# set flexible-vlan-tagging mtu 9192 encapsulation
flexible-ethernet-services
```

6. Configure a logical unit for the interface and specify the encapsulation and configure the VLAN ID on the logical interfaces.

```
[edit interfaces ge-0/2/0]
user@host# set unit 0 encapsulation vlan-bridge vlan-id 512
```

7. Configure the bridge domain, bd1, and specify the VLAN ID associated with the bridge domain and the associated interfaces from the **[edit]** hierarchy level.

```
[edit]
user@host# set bridge-domains bd1 vlan-id 10 interface ge-0/2/1.0
user@host# set bridge-domains bd1 vlan-id 10 interface ge-0/2/0.0
```

### Configuring the VPLS Parameters on the MX Series Router (PE1)

#### Step-by-Step Procedure

The following configuration requires you to enable a simple VPLS topology between the PE1 and PE2 routers. In this example, PE1 is a MX Series router. On the PE1 router, configure the tunnel services interface and prepare the router for VPLS by configuring the BGP, MPLS, OSPF protocols.

To configure the VPLS parameters on the MX Series Router:

1. Configure tunnel services.

```
[edit]
user@host# set chassis fpc 0 pic 2 tunnel-services
```

2. Configure the VPLS VLAN encapsulation on the router.

```
[edit interfaces]
user@host# set interfaces ge-0/2/1 flexible-vlan-tagging
user@host# set interfaces ge-0/2/1 mtu 9192
user@host# set interfaces ge-0/2/1 encapsulation vlan-vpls
user@host# set interfaces ge-0/2/1 unit 0 encapsulation vlan-vpls
user@host# set interfaces ge-0/2/1 unit 0 vlan-id 512
```

3. Configure the routing interface and the loopback interface on the router.

```
[edit interfaces]
user@host# set interfaces ge-0/3/0 mtu 9192
user@host# set interfaces ge-0/3/0 unit 0 family inet address 32.0.0.1/24
user@host# set interfaces ge-0/3/0 unit 0 family mpls
user@host# set interfaces lo0 unit 0 family inet address 100.1.1.1/32
```

4. Configure the routing options on the router.

```
[edit routing-options]
user@host# set routing-options router-id 100.1.1.1
user@host# set routing-options autonomous-system 100
```

5. Configure MPLS on the router to advertise the Layer 2 VPN interface that communicates with the PE2 router.

```
[edit protocols]
user@host# set protocols mpls interface ge-0/3/0.0
```

6. Configure BGP as the signaling protocol on the router to enable carrying of Layer 2 VPLS messages.

```
[edit protocols]
user@host# set protocols bgp group test type internal
user@host# set protocols bgp group test local-address 100.1.1.1
user@host# set protocols bgp group test family l2vpn signaling
user@host# set protocols bgp group test neighbor 100.1.1.2
```

7. Configure OSPF on the router to enable exchange of routing information.

```
[edit protocols]
user@host# set protocols ospf traffic-engineering
user@host# set protocols ospf reference-bandwidth 1g
user@host# set protocols ospf area 0.0.0.0 interface ge-0/3/0.0
user@host# set protocols ospf area 0.0.0.0 interface lo0.0
```

8. Configure LDP on the router to enable LDP for all connections

```
[edit protocols]
user@host# set protocols ldp interface ge-0/3/0.0
user@host# set protocols ldp interface lo0.0
```

9. Create and configure the VPLS routing interface.

```
[edit routing instances vpls-instance]
user@host# set routing-instances vpls-pe1 instance-type vpls
user@host# set routing-instances vpls-pe1 interface ge-0/2/1.0
user@host# set routing-instances vpls-pe1 no-local-switching
user@host# set routing-instances vpls-pe1 route-distinguisher 100.1.1.1:101
user@host# set routing-instances vpls-pe1 vrf-target target:1:2
user@host# set routing-instances vpls-pe1 protocols vpls site-range 8
user@host# set routing-instances vpls-pe1 protocols vpls no-tunnel-services
user@host# set routing-instances vpls-pe1 protocols vpls site HUB site-identifier 1
user@host# set routing-instances vpls-pe1 protocols vpls vpls-id 1
user@host# set routing-instances vpls-pe1 protocols vpls neighbor 100.1.1.2
```

### Configuring Benchmarking Test Parameters on the MX104 Router (Reflector)

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

The following configuration requires you to configure a unique test-name for the benchmarking test on the MX104 router. The test-name defines the parameters for the benchmarking test to be performed. Because the test interface and test MAC addresses are the same, you can create a single test configuration at the reflector (MX104).

To configure the benchmarking test parameters on the MX104 Router:

1. In configuration mode, at the **[edit]** hierarchy level, configure a real-time performance monitoring service (RPM) instance and an RFC2544-based benchmarking test for the RPM instance.

```
[edit]
user@host# edit services rpm rfc2544-benchmarking
```

2. Define a name for the test—for example, l2v-reflector. The test name can be up to 32 characters in length.

```
[edit services rpm rfc2544-benchmarking]
user@host# edit tests test-name l2v-reflector
```

3. Specify the source and destination MAC addresses of the test packet.  

```
[edit services rpm rfc2544-benchmarking test-name l2v-reflector]
user@host# set source-mac-address 00:00:00:00:11:11 destination-mac-address
00:00:00:00:22:22
```
4. Specify the service type under test and the mode in which the test is executed, which is in-service, at the reflector. Also, specify if the IP address, TCP and UDP port must be swapped.  

```
[edit services rpm rfc2544-benchmarking test-name l2v-reflector]
user@host# set service-type elan in-service ip-swap udp-tcp-port-swap
```
5. Specify the mode which is reflect at the reflector.  

```
[edit services rpm rfc2544-benchmarking test-name l2v-reflector]
user@host# set mode reflect
```
6. Configure the family type, **vppls**, specify the direction, egress, and specify the protocol being transported in the Ethernet frame, for the benchmarking test. Also, specify the source and destination UDP ports and specify the logical interface, ge-0/3/1.0, on which the RFC2544-based benchmarking test is being run.  

```
[edit services rpm rfc2544-benchmarking tests test-name l2v-reflector]
user@host# set family vppls direction egress source-udp-port 200 destination-udp-port
200 test-interface ge-0/3/1.0
```

### Configuring Other Benchmarking Test Parameters on the MX104 Router (Reflector)

#### 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.

To configure the interface and bridge domain on the MX104 Router:

1. Configure the Layer 2 NNI interface on which the tests must be run.  

```
[edit]
user@host# edit interfaces ge-0/3/1.0
```
2. Configure flexible VLAN tagging for transmission of untagged frames or 802.1Q single-tagged and dual-tagged frames on the logical interface. You can also specify the maximum transmission unit (MTU) size for the interface and the encapsulation.  

```
[edit interfaces ge-0/3/1.0]
user@host# set flexible-vlan-tagging mtu 9192 encapsulation vlan-vpls
```
3. Configure a logical unit for the interface, specify the encapsulation, and configure the VLAN ID on the logical interface.  

```
[edit interfaces ge-0/3/1.0]
user@host# set unit 0 encapsulation vlan-vpls vlan-id 512
```
4. Configure the Layer 2 UNI interface.  

```
[edit]
user@host# edit interfaces ge-0/3/2.0
```

5. Configure flexible VLAN tagging for transmission of untagged frames or 802.1Q single-tagged and dual-tagged frames on the logical interface. You can also specify the maximum transmission unit (MTU) size for the interface and the encapsulation.

```
[edit interfaces ge-0/3/2.0]
user@host# set flexible-vlan-tagging mtu 9192 encapsulation vlan-vpls
```

6. Configure a logical unit for the interface, specify the encapsulation, and configure the VLAN ID on the logical interfaces.

```
[edit interfaces ge-0/3/2.0]
user@host# set unit 0 encapsulation vlan-vpls vlan-id 512
```

7. `/**Configure the bridge domain, bd1, and specify the VLAN ID associated with the bridge domain, and the associated interfaces from the [edit] hierarchy level.`

```
[edit]
user@host# set bridge-domains bd1 vlan-id 500 interface ge-1/1/6.0
user@host# set bridge-domains bd1 vlan-id 500 interface ge-1/1/5.0 **//
```

8. Start the benchmarking test on the reflector.

```
user@host> test services rpm rfc2544-benchmarking test l2v-reflector 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 l2v-reflector stop** command.

### Configuring VPLS Parameters on the MX104 Router (Reflector)

#### Step-by-Step Procedure

The following configuration requires you to enable a simple VPLS topology between the PE1 and PE2 routers. In this example, PE2 is a MX104 router. On the PE2 router, configure the tunnel services interface and prepare the router for VPLS by configuring the BGP, MPLS, OSPF protocols to complement the configuration on PE1.

1. Configure tunnel services.

```
[edit]
user@host# set chassis fpc 0 pic 2 tunnel-services
```

2. Configure the VPLS VLAN encapsulation on the router.

```
[edit interfaces]
user@host# set interfaces ge-0/2/5 flexible-vlan-tagging
user@host# set interfaces ge-0/2/5 mtu 9192
user@host# set interfaces ge-0/2/5 encapsulation vlan-vpls
user@host# set interfaces ge-0/2/5 unit 0 encapsulation vlan-vpls
user@host# set interfaces ge-0/2/5 unit 0 vlan-id 512
```

3. Configure the routing interface and the loopback interface on the router.

```
[edit interfaces]
user@host# set interfaces ge-0/3/0 mtu 9192
user@host# set interfaces ge-0/3/0 unit 0 family inet address 32.0.0.1/24
user@host# set interfaces ge-0/3/0 unit 0 family mpls
user@host# set interfaces lo0 unit 0 family inet address 100.1.1.1/32
```

4. Configure the routing options on the router.



```
[edit routing-options]
user@host# set routing-options router-id 100.1.1.1
user@host# set routing-options autonomous-system 100
```

5. Configure MPLS on the router to advertise the Layer 2 VPN interface that communicates with the PE1 router.

```
[edit protocols]
user@host# set protocols mpls interface ge-0/2/5.0
```

6. Configure BGP as the signaling protocol on the router to enable carrying of Layer 2 VPLS messages.

```
[edit protocols]
user@host# set protocols bgp group test type internal
user@host# set protocols bgp group test local-address 100.1.1.1
user@host# set protocols bgp group test family l2vpn signaling
user@host# set protocols bgp group test neighbor 100.1.1.2
```

7. Configure OSPF on the router to enable exchange of routing information.

```
[edit protocols]
user@host# set protocols ospf traffic-engineering
user@host# set protocols ospf reference-bandwidth 1g
user@host# set protocols ospf area 0.0.0.0 interface ge-0/2/5.0
user@host# set protocols ospf area 0.0.0.0 interface lo0.0
```

8. Configure LDP on the router to enable LDP for all interfaces.

```
[edit protocols]
user@host# set protocols ldp interface ge-0/2/5.0
user@host# set protocols ldp interface lo0.0
```

9. Create and configure the VPLS routing interface.

```
[edit routing instances vpls-instance]
user@host# set routing-instances vpls-pe2 instance-type vpls
user@host# set routing-instance vpls-pe2 interface ge-0/3/1.0
user@host# set routing-instances vpls-pe2 no-local-switching
user@host# set routing-instances vpls-pe2 route-distinguisher 100.1.1.1:101
user@host# set routing-instances vpls-pe2 vrf-target target:1:2
user@host# set routing-instances vpls-pe2 protocols vpls site-range 8
user@host# set routing-instances vpls-pe2 protocols vpls no-tunnel-services
user@host# set routing-instances vpls-pe2 protocols vpls site SPOKE site-identifier
1
user@host# set routing-instances vpls-pe2 protocols vpls vpls-id 1
user@host# set routing-instances vpls-pe2 protocols vpls neighbor 100.1.1.2
```

## Results

In configuration mode, confirm your configuration on the ACX Router, the MX Series router, and the MX104 Router 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 the ACX Router :

```
[edit interfaces]
ge-0/2/0 {
```

```

 flexible-vlan-tagging;
 mtu 9192;
 encapsulation flexible-ethernet-services;
 unit 0 {
 encapsulation vlan-bridge;
 vlan-id 512;
 }
 }
 ge-0/2/1 {
 flexible-vlan-tagging;
 mtu 9192;
 encapsulation flexible-ethernet-services;
 unit 0 {
 encapsulation vlan-bridge;
 vlan-id 512;
 }
 }
 }

[edit bridge-domains]
bd1 {
 vlan-id 600;
 interface ge-0/2/1.0;
 interface ge-0/2/0.0;
}

[edit services rpm]
rfc2544-benchmarking {
 profiles {
 test-profile tput {
 test-type throughput
 packet-size 256;
 bandwidth-kbps 600000;
 }
 test-profile b2bt {
 test-type back-back-frames
 packet-size 9104;
 bandwidth-kbps 600000;
 }
 test-profile lty {
 test-type latency
 packet-size 1024;
 bandwidth-kbps 600000;
 }
 test-profile frloss {
 test-type frameloss
 packet-size 1600;
 bandwidth-kbps 6000000;
 }
 }

 tests {
 test-name tput-test {
 interface ge-0/2/0.0;
 test-profile tput;
 mode initiate,terminate;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 }
 ovlan-id 512;
 service-type elan;
 family bridge;
 direction egress;
 }
}

```

```

 source-udp-port 200;
 destination-udp-port 400;
 test-iterator-duration 250;
 }
test-name b2b-test {
 interface ge-0/2/0.0;
 test-profile b2bt;
 mode initiate,terminate;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 ovlan-id 512;
 service-type elan;
 family bridge;
 direction egress;
 destination-udp-port 400;
 test-iterator-duration 10;
 }
test-name lty-test {
 interface ge-0/2/0.0;
 test-profile lty;
 mode initiate,terminate;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 ovlan-id 512;
 service-type elan;
 family bridge;
 direction egress;
 source-udp-port 200;
 destination-udp-port 400;
 test-iterator-duration 10;
 }
test-name frloss-test {
 interface ge-0/2/0.0;
 test-profile frloss;
 mode initiate,terminate;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 ovlan-id 512;
 service-type elan;
 family bridge;
 direction egress;
 source-udp-port 200;
 destination-udp-port 400;
 test-iterator-duration 30;
 }
}

```

#### VPLS Parameters on the MX Router:

```

[edit routing-instances]
vpls-instance {
 instance-type vpls;
 interface ge-0/2/1.0;
 route-distinguisher 100.1.1.1:101;
 vrf-target target:1:2;
}
protocols {
 vpls {
 vpls-id 1;
 }
}

```

```
neighbor 100.1.1.2;
site-range 8;
no-tunnel-services;
site HUB {
site-identifier 1;
}
```

Benchmarking Test Parameters and VPLS Parameters on the MX104 Router:

```
[edit interfaces]
 ge-0/3/1 {
 flexible-vlan-tagging;
 mtu 9192;
 encapsulation vlan-vpls;
 unit 0 {
 encapsulation vlan-vpls;
 vlan-id 512;
 }
 }
 ge-0/2/5 {
 flexible-vlan-tagging;
 mtu 9192;
 unit 0 {
 family inet address 42.0.0.1/24;
 family mpls;
 }
 }

[edit services rpm]
rfc2544-benchmarking {
 # Note, When in reflector mode, test profile is not needed
 tests {
 test-name l2v-reflector {
 interface ge-0/3/1.0;
 source-mac-address 00:00:00:00:11:11;
 destination-mac-address 00:00:00:00:22:22;
 }
 }
 mode reflect;
 service-type elan;
 in-service;
 ip-swap;
 udp-tcp-port swap;
 family vpls;
 reflect-etype 2048;
 direction egress;
 source-udp-port 200;
 destination-udp-port 200;
}

[edit routing-instances]
vpls-instance {
 instance-type vpls;
 interface ge-0/3/1;
 route-distinguisher 100.1.1.2:102;
 vrf-target target:1:2;
}
protocols {
 vpls {
 vpls-id 1;
 }
}
```

```
neighbor 100.1.1.1;
site-range 8;
no-tunnel-services;
site SPOKE {
site-identifier 2;
}
```

After you have configured the device, enter the **commit** command, in configuration mode.

## Verifying the Results of the Benchmarking Test for Layer 2 ELAN Services Using VPLS

Examine the results of the benchmarking test that is performed on the configured service between the ACX router and the MX104 router.

- [Verifying the Benchmarking Test Results on page 307](#)

---

### 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 the ACX router and the MX104 router.                                                                                                                                                                                                                                                                           |
| <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 CLI Explorer.                                                                                                                                                                                                         |
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li><li>• <a href="#">Example: Configuring RFC2544-Based Benchmarking Tests for Layer 2 E-LAN Services in Bridge Domains on page 262</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">Supported RFC2544-Based Benchmarking Statements on MX104 Routers on page 234</a></li></ul> |



# Tracking Streaming Media Traffic Using Inline Video Monitoring

- [Inline Video Monitoring Overview on page 309](#)
- [Configuring Inline Video Monitoring on page 311](#)
- [Inline Video Monitoring Syslog Messages on page 314](#)
- [Generation of SNMP Traps and Alarms for Inline Video Monitoring on page 314](#)
- [SNMP Traps for Inline Video Monitoring Statistics on page 317](#)
- [Processing SNMP GET Requests for MDI Metrics on page 318](#)

## Inline Video Monitoring Overview

---

Junos OS supports inline video monitoring using Media Delivery Index (MDI) metrics.

Before you use the inline video monitoring feature, ensure that you understand the following terms:

- **media delivery index**—MDI metrics facilitate identification of buffering needs for streaming media. Buffering must be adequate to compensate for packet jitter, measured by the MDI delay factor, and quality problems indicated by lost packets, measured by the MDI media loss rate (MLR). By performing measurements under varying load conditions, you can identify sources of significant jitter or packet loss and take appropriate action.
- **delay factor** —Delay factor is the maximum observed time difference between the arrival of media data and the drain of media data. The expected drain rate is the nominal, constant traffic rate for constant bit rate streams or the computed traffic rate of variable rate media stream packet data.

For typical stream rates of 1 megabit per second and higher, an interval of one second provides an adequate sample time. The delay factor indicates how long a data stream must be buffered (delayed) at its nominal bit rate to prevent packet loss.

The delay factor suggests the minimum size of the buffer required at the next downstream node. As a stream progresses, the variation of the delay factor indicates packet bunching or packet gaps (jitter). Greater delay factor values also indicate that more network latency is needed to deliver a stream due to the need to pre-fill a receive buffer before beginning the drain to guarantee no underflow.

When the nominal drain bit rate at a receiving node is known, the delay factor's maximum indicates the size of buffer required to accommodate packet jitter.

- **Media rate variation (MRV)**—This value is the difference between the expected packet rate and actual packet rate expressed as a percentage of the expected packet rate.
- **Media loss rate (MLR)**—This value is the number of media packets lost over a configurable time interval (*interval-duration*,) where the flow packets are packets carrying streaming application information. A single IP packet can contain zero or more streaming packets. For example, an IP packet typically contains seven 188-byte MPEG transport stream packets. In this case, a single IP packet loss results in seven lost packets counted (if those seven lost packets did not include null packets). Including out-of-order packets is important, because many stream consumer-type devices do not attempt to reorder packets that are received out of order.

To configure the monitoring process, define criteria templates and apply them to the interfaces and flows you want to monitor. Monitoring templates include the following criteria:

- Duration of each measurement cycle
- Flow rate information used to establish expected flow rates
- Threshold levels for media rate variation and media loss rate that trigger desired syslog alerts

For each interface you want to monitor, you can define one or more filters to select flows for monitoring. Flows are designated as input or output flows and are uniquely identified by:

- Source IP address
- Source port
- Destination IP address
- Destination port

Junos OS supports the definition of filters for up to 256 flows, which can consist of input flows, output flows, or a combination of input and output flows. These filters provide criteria for selecting flows for monitoring. If the selection criteria consist of lists of IP addresses or ports, you could exceed the maximum number of match conditions for flows. Video monitoring selects a widely variable number of flows based on flow filters.

Inline video monitoring is available on MX Series 3D Universal Edge Routers using only the following MPCs:

- MPCE1
- MPCE2
- MPC-16XGE

The total number of flows that can be measured at a time depends on the specific MPC being used, as shown in [Table 31 on page 311](#).



When you do not define input or output flow filters for a monitored interfaces, all flows on the interface are subject to monitoring.

**Table 31: MPC Flow Monitoring Capacity by Model**

| MPC Model | Maximum Number of Flows Monitored Simultaneously |
|-----------|--------------------------------------------------|
| MPCE1     | 1000                                             |
| MPCE2     | 2000                                             |
| MPC-16XGE | 4000                                             |



**NOTE:** Junos OS measures both UDP flows (the default) and RTP flows. Junos OS differentiates media traffic over UDP or RTP by inspecting the first byte in the UDP payload. If the first byte of the UDP payload is 0x47 (MPEG2-TS sync byte), the traffic is treated as media traffic over UDP. Traffic is treated as media traffic over RTP if the version field is 2 and the payload type is 33 in the RTP header. When neither of these criteria are met, the packet is not considered for video monitoring.

Starting in Junos OS Release 15.1, MX Series routers support the inline video monitoring to measure media delivery index (MDI) metrics that can be accessed using the SNMP GET operation. Currently, inline MDI can generate only a system log when the computed value is not within the configured range. SNMP is primarily used to monitor alarms raised by the inline video monitoring feature. The alarms are monitored in the network management systems either to troubleshoot the problem or to diagnose degradation in video quality.

You use the **video-monitoring** statement at the **[edit services]** hierarchy level to specify monitoring criteria for two key indicators of video traffic problems: delay factor and media loss rate (MLR), and to apply these metrics to flows on designated interfaces.

**Related Documentation**

- [Configuring Inline Video Monitoring on page 311](#)
- [show services video-monitoring mdi stats fpc-slot on page 687](#)
- [show services video-monitoring mdi errors fpc-slot on page 681](#)
- [show services video-monitoring mdi flows fpc-slot on page 683](#)
- [alarms on page 342](#)

## Configuring Inline Video Monitoring

To configure inline video monitoring, perform the following tasks.

- [Configuring Media Delivery Indexing Criteria on page 312](#)
- [Configuring Interface Flow Criteria on page 313](#)

## Configuring Media Delivery Indexing Criteria

To configure media delivery indexing criteria:

1. In edit mode, create a named template for video monitoring.

```
user@host# edit services video-monitoring templates template-name
```

For example,

```
user@host# edit services video-monitoring templates t1
```

2. Set the duration for sampling in seconds. Flow media delivery indexing statistics are updated at the end of this interval.

```
[edit services video-monitoring templates t1]
user@host# set interval-duration 1
```



**BEST PRACTICE:** If you change the interval duration when a template is being used, you cause a change in the calculated number of expected packets in an measurement interval for the template. We recommend that you do not change the interval duration for a template that is in use.

3. Set the inactivity timeout.

```
[edit services video-monitoring templates t1]
user@host# set inactivity-timeout 30
```

4. Configure either **media-rate** or **layer3-packet-rate** to establish expected flow rates used to compare to monitored flow rates.



**NOTE:** The media rate is the configured media bit rate for the stream. The media rate is used to establish *expected packets per second (pps)*.

The layer 3 packet rate in packets per second (pps) and is used to establish *expected bits per second (bps)*.

```
[edit services video-monitoring templates t1]
user@host# set media-rate 2972400
```

5. Set delay factor thresholds for syslog message levels.

```
[edit services video-monitoring templates t1]
user@host# set delay-factor threshold info 100
user@host# set delay-factor threshold warning 200
user@host# set delay-factor threshold critical 300
```

6. Set media loss rate thresholds for syslog message levels. You can set the threshold based on number of packets lost, or percentage of packets lost.

Or

```
[edit services video-monitoring templates t1]
user@host# set media-loss-rate threshold info percentage 5
user@host# set media-loss-rate threshold warning percentage 10
```

```
user@host# set media-loss-rate threshold critical percentage 20
```

7. Set the media rate variation thresholds for syslog message levels. The threshold is based on the ratio of the *difference* between the configured media rate and the monitored media rate to the configured media rate, expressed as a percentage.

```
[edit services video-monitoring templates t1]
user@host# set media-rate-variation threshold info 10
user@host# set media-rate-variation threshold warning 15
user@host# set media-rate-variation threshold critical 20
```

## Configuring Interface Flow Criteria

To configure monitoring of flows for interfaces:

1. In edit mode, identify an interface for monitoring .

```
user@host# edit services video-monitoring interfaces interface-name
```

2. Identify input flows for monitoring. Flows are uniquely identified by source IP address, source port, destination IP address, and destination port. You can restrict flow measurement by specifying values for these identifiers. You can specify individual addresses or ports or lists of addresses and ports. If you do not specify any identifiers, all flows on the interface are monitored.

```
[edit services video-monitoring interfaces interface-name]
user@host# set input-flows input-flow-name
user@host# set input-flows input-flow-name source-address address
user@host# set input-flows input-flow-name source-port port
user@host# set input-flows input-flow-name destination-address address
user@host# set input-flows input-flow-name destination-port port
```



**NOTE:** You can configure a maximum of 256 flow definitions. If your flow definitions contain lists of addresses and ports, you may exceed the number of match conditions. When you exceed the limits for flows or match conditions, you receive the following constraint message when you commit:

```
'interfaces xe-0/2/2.0'
 Number of flows or Number of match condition under flows exceeded
 limit
error: configuration check-out failed
```

3. Identify output flows for monitoring, using the same options listed in Step 2.
4. Identify the template used to monitor the flows on the interface.

```
[edit services video-monitoring interfaces interface-name]
set template t1
```

### Related Documentation

- [Inline Video Monitoring Overview on page 309](#)
- [templates on page 504](#)
- [interfaces on page 417](#)

## Inline Video Monitoring Syslog Messages

---

The following examples show the syslog messages produced when configured video monitoring thresholds are exceeded.

### `/var/log/messages`

```
Mar 11 18:36:25 tstrtr01 fpc2 [MDI] DF: 56.71 ms, exceeded threshold for
flow(src:20.0.0.2 dst:30.0.0.2 sport:1024 dport:2048) ingressing at interface
xe-2/2/1.0 with template t1.
Mar 11 18:36:25 tstrtr01 fpc2 [MDI] MLR : 112, exceeded threshold for flow
(src:20.0.0.2 dst:30.0.0.2 sport:1024 dport:2048) ingressing at interface
xe-2/2/1.0 with template t1.
Mar 11 18:36:25 tstrtr01 fpc2 [MDI] MRV : -5.67, exceeded threshold for flow
(src:20.0.0.2 dst:30.0.0.2 sport:1024 dport:2048) ingressing at interface
xe-2/2/1.0 with template t1.
```

### Console Messages

```
NPC2(tstrtr01 vty)# [Mar 12 01:40:58.411 LOG: Critical] [MDI] MLR : 420, exceeded
threshold for flow (src:20.0.0.2 dst:30.0.0.2 sport:1024 dport:2048) ingressing
at interface xe-2/2/1.0 with template t1.
[Mar 12 01:40:58.411 LOG: Critical] [MDI] MRV : -14.89, exceeded threshold for
flow (src:20.0.0.2 dst:30.0.0.2 sport:1024 dport:2048) ingressing at interface
xe-2/2/1.0 with template t1.
[Mar 12 01:40:59.412 LOG: Critical] [MDI] DF: 141.74 ms, exceeded threshold for
flow(src:20.0.0.2 dst:30.0.0.2 sport:1024 dport:2048) ingressing at interface
xe-2/2/1.0 with template t1.
```

**Related Documentation**

- [Configuring Inline Video Monitoring on page 311](#)

## Generation of SNMP Traps and Alarms for Inline Video Monitoring

---

Starting in Junos OS Release 15.1, SNMP support is introduced for the Media Delivery Index (MDI) metrics of inline video monitoring. Inline video monitoring is available on MX Series routers using only MPCE1, MPCE2, and MPC- 16XGE. Until Junos OS Release 14.2, inline MDI generated only syslogs when the computed MDI metric value was not within the configured range. SNMP support is now added to enable SNMP traps to be triggered when the computed delay factor (DF), media rate variation (MRV), and media loss rate (MLR) value is not within the configured range. You can retrieve the MDI statistics, flow levels, error details, and MDI record-level information using SNMP Get and Get Next requests. The SNMP traps and alarms that are generated when the MDI metrics exceed the configured ranges can be cleared as necessary. Also, you can control the flooding of SNMP traps on the system.

The following sections describe the statistical counters and parameters that are collected for MDI records and for generation of SNMP traps and alarms when the DF, MRV, and MLR values are not within the specified ranges.

## Collection of MDI Statistics Associated with an FPC Slot

The FPC-level statistics include the following parameters that are displayed in the output of the **show services video-monitoring mdi stats fpc-slot *fpc-slot*** command. All of these attributes can be obtained using the SNMP Get request.

**Table 32: show services video-monitoring mdi stats fpc-slot Output Fields**

| Field Name                  | Field Description                                                                                                                                                                              |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FPC Slot</b>             | Slot number of the monitored FPC                                                                                                                                                               |
| <b>Active Flows</b>         | Number of active flows currently monitored.<br>active flows = inserted flows - deleted flows.                                                                                                  |
| <b>Total Inserted Flows</b> | Number of flows initiated under video monitoring.                                                                                                                                              |
| <b>Total Deleted Flows</b>  | Number of flows deleted due to inactivity timeout.                                                                                                                                             |
| <b>Total Packets Count</b>  | Number of total packets monitored.                                                                                                                                                             |
| <b>Total Bytes Count</b>    | Number of total bytes monitored.                                                                                                                                                               |
| <b>DF Alarm Count</b>       | Number of delay factor alarms at each of the following levels: <ul style="list-style-type: none"> <li>• Info level</li> <li>• Warning level</li> <li>• Critical level</li> </ul>               |
| <b>MLR Alarm Count</b>      | Number of media loss rate (MLR) alarms at each of the following levels: <ul style="list-style-type: none"> <li>• Info level</li> <li>• Warning level</li> <li>• Critical level</li> </ul>      |
| <b>MRV alarm count</b>      | Number of media rate variation (MRV) alarms at each of the following levels: <ul style="list-style-type: none"> <li>• Info level</li> <li>• Warning level</li> <li>• Critical level</li> </ul> |

## Collection of MDI Errors Associated with an FPC Slot

The FPC-level statistics include the following parameters that are displayed in the output of the **show services video-monitoring mdi errors fpc-slot *fpc-slot*** command. All of these attributes can be obtained using the SNMP Get request.

Table 33: show services video-monitoring mdi errors fpc-slot Output Fields

| Field Name                      | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FPC slot                        | Slot number of the monitored FPC.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Flow Insert Error               | Number of errors during new flow insert operations.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Flow Policer Drops              | Number of packets dropped by flow policer process.<br><br><b>NOTE:</b> New flows usually arrive within a very short time interval (1.5 microseconds). These errors do not represent the loss of entire flows, because subsequent packets in the flow can establish the flow. All packets are monitored after a flow has been established. Packet forwarding occurs independently of the video monitoring, and packets are not dropped due to video monitoring errors. |
| Unsupported Media Packets Count | Number of packets dropped because they are not media packets or they are unsupported media packets.                                                                                                                                                                                                                                                                                                                                                                   |
| PID Limit Exceeded              | Number of packets unmonitored because the process identifier (PID) limit exceeded has been exceeded.<br><br><b>NOTE:</b> The current PID limit is 6.                                                                                                                                                                                                                                                                                                                  |

### Collection of MDI Flows Associated with an FPC Slot

The FPC-level statistics include the following parameters that are displayed in the output of the **show services video-monitoring mdi flows fpc-slot fpc-slot** command. All of these attributes can be obtained using the SNMP Get request.

Table 34: show services mdi flows Output Fields

| Field Name  | Field Description                                                          |
|-------------|----------------------------------------------------------------------------|
| SIP         | Source IP address                                                          |
| DIP         | Destination IP address                                                     |
| SP          | Source port                                                                |
| DP          | Destination port                                                           |
| Di          | Direction (I=Input, O=Output)                                              |
| Ty          | Type of flow                                                               |
| Last DF:MLR | Delay factor and media loss rate value of last media delivery index record |
| Avg DF:MLR  | Average value of delay factor and media loss rate                          |
| Last MRV    | Media rate variation value of last media delivery index record             |

Table 34: show services mdi flows Output Fields (*continued*)

| Field Name    | Field Description                         |
|---------------|-------------------------------------------|
| Avg MRV       | Average value of media rate variation     |
| IFL           | Interface name on which flow is receiving |
| Template Name | Name of template associated with flow     |

## Collection of MDI Record-Level Metrics

The computed DF, MLR, and MRV counters of all valid MDI records of a flow that you can view by using the output of the show services video-monitoring mdi flow fpc-slot fpc-slot detail command can be obtained by using the SNMP Get request.

Related  
Documentation

## SNMP Traps for Inline Video Monitoring Statistics

SNMP is primarily used to monitor alarms raised by the inline video monitoring feature. The alarms sent to a network management system (NMS) either to troubleshoot the problem quickly or to proactively diagnose degradation in video quality. The following SNMP traps or alarms are implemented with the Cleared, Info, Warning, and Critical severity levels. The Cleared severity level is used to indicate a normal condition and to clear a particular alarm. Whenever a change in the alarm level occurs, the corresponding alarm is generated.

All the alarms include the following information pertaining to the MDI flows:

- Source IP address
- Destination IP address
- Source Port Destination
- Port Traffic type (UDP or RTP)
- Computed DF, MLR, and MRV values

The following traps are generated for MDI metrics:

- mdiMLRAlarm—This trap is generated when the computed MLR value is not within the configured range.
- mdiDFAlarm—This trap is generated when the computed DF value is not within the configured range.
- mdiMRVAlarm—This trap is generated when the computed MRV value is not within the configured range.

To enable the generation of SNMP traps or alarms for inline video monitoring or MDI metrics, include the **alarms** statement and its substatements at the **[edit services video-monitoring]** hierarchy level.

**Related** •  
**Documentation**

---

## Processing SNMP GET Requests for MDI Metrics

---

A query on-demand mechanism without caching facility is used to process the SNMP Get requests. The Routing Engine queries the Packet Forwarding Engine to obtain the computed metrics on every Get request. The Routing Engine does not maintain computed metrics locally. No additional memory is required to cache queried metrics. The network management system (NMS) server can receive latest information on every Get request, especially regarding the MDI records because MDI records are updated very frequently. However, querying the Packet Forwarding Engine PFE on each GET request is resource-consuming if the volume of metrics is large. The response to a Get request might be relatively delayed as the Routing Engine has to poll the Packet Forwarding Engine to obtain the metrics.

Inline MDI metrics are real-time data where cached information might not be valid. Reporting cached or invalid metrics is not beneficial because it is a real-time monitoring feature. An increase in the number of flows and number of MDI records per flow causes a proportional increase in the volume of memory required in the Routing Engine to store flows and MDI records for all flows. Because asynchronous traps are generated for threshold with enough contents, frequent Get request from NMS are not highly expected, reducing the periodicity of polling to the Packet Forwarding Engine. SNMP traps are triggered with the severity level of Info, Warning, Critical, or Cleared. A trap with the cleared severity level is used to clear an alarm.

Whenever a change in the alarm level occurs, the designated trap is triggered. For example, if the delay factor (DF) alarm changes from informational level to warning level, or from warning to critical, the mdiDFAlarm trap is triggered. Alarm can be immediate or average. If the immediate alarm is configured, an immediate trap is raised at the end of interval duration if the metric value exceeds the configured range. If the average alarm is configured, a trap is generated, based on the average value for specified number of interval duration.

Storm control is applied for SNMP traps at the flow level and not at the FPC level. The NMS system can obtain SNMP trap from all the flows even if multiple flows are generating traps at approximately the same time. If multiple flows are generating traps at nearly the same time, NMS is flooded by many traps at the same time. For example, no traffic received on a logical interface owing to any reason can trigger all alarms and cause an avalanche of alarms on the NMS server.

**Related** •  
**Documentation**



## PART 5

# Configuration Statements and Operational Commands

- [Configuration Statements on page 321](#)
- [Operational Commands on page 535](#)



## CHAPTER 15

# Configuration Statements

- [\[edit forwarding-options\] Hierarchy Level on page 328](#)
- [\[edit interfaces\] Hierarchy Level on page 331](#)
- [\[edit services dynamic-flow-control\] Hierarchy Level on page 332](#)
- [\[edit services flow-collector\] Hierarchy Level on page 333](#)
- [\[edit services flow-monitoring\] Hierarchy Level on page 334](#)
- [\[edit services flow-tap\] Hierarchy Level on page 335](#)
- [\[edit services rpm\] Hierarchy Level on page 335](#)
- [accounting on page 338](#)
- [address \(Interfaces\) on page 339](#)
- [address \(Services Dynamic Flow Capture\) on page 339](#)
- [aggregate-export-interval on page 340](#)
- [aggregation on page 341](#)
- [alarms on page 342](#)
- [alarm-mode on page 343](#)
- [allowed-destinations on page 344](#)
- [analyzer-address on page 344](#)
- [analyzer-id on page 345](#)
- [archive-sites on page 345](#)
- [authentication-mode on page 346](#)
- [authentication-key-chain \(TWAMP\) on page 347](#)
- [autonomous-system-type on page 348](#)
- [bgp on page 349](#)
- [capture-group on page 350](#)
- [cflowd \(Discard Accounting\) on page 351](#)
- [cflowd \(Flow Monitoring\) on page 352](#)
- [client on page 353](#)
- [client-list on page 354](#)
- [collector on page 354](#)

- [collector \(Flow Monitoring Logs for NAT\)](#) on page 355
- [collector \(Flow Template Profiles for NAT\)](#) on page 356
- [collector-group \(Flow Template Profiles for NAT\)](#) on page 357
- [collector-group \(Flow Monitoring Logs for NAT\)](#) on page 358
- [content-destination](#) on page 359
- [control-connection](#) on page 360
- [control-source](#) on page 361
- [core-dump](#) on page 362
- [data-fill](#) on page 363
- [data-fill-with zeros](#) on page 364
- [data-format](#) on page 364
- [data-size](#) on page 365
- [delay-factor](#) on page 366
- [destination \(Interfaces\)](#) on page 367
- [destination-address \(Flow Monitoring Logs for NAT\)](#) on page 368
- [destination-interface](#) on page 369
- [destination-ipv4-address \(RFC 2544 Benchmarking\)](#) on page 370
- [destination-mac-address \(RFC2544 Benchmarking\)](#) on page 371
- [destination-port](#) on page 372
- [destination-port \(Flow Monitoring Logs for NAT\)](#) on page 373
- [destination-udp-port \(RFC 2544 Benchmarking\)](#) on page 373
- [destinations](#) on page 374
- [direction \(RFC2544 Benchmarking\)](#) on page 375
- [disable \(Forwarding Options\)](#) on page 376
- [disable-signature-check \(RFC 2544 Benchmarking\)](#) on page 377
- [dscp-code-point](#) on page 378
- [duplicates-dropped-periodicity](#) on page 379
- [dynamic-flow-capture](#) on page 380
- [engine-id \(Forwarding Options\)](#) on page 381
- [engine-type](#) on page 382
- [export-format](#) on page 383
- [extension-service](#) on page 384
- [family \(Monitoring\)](#) on page 386
- [family \(Port Mirroring\)](#) on page 387
- [family \(RFC2544 Benchmarking\)](#) on page 388
- [family \(Sampling\)](#) on page 389
- [file \(Sampling\)](#) on page 390

- [file \(Trace Options\) on page 391](#)
- [file-specification \(File Format\) on page 391](#)
- [file-specification \(Interface Mapping\) on page 392](#)
- [filename on page 392](#)
- [filename-prefix on page 393](#)
- [files on page 393](#)
- [filter on page 394](#)
- [flow-active-timeout on page 395](#)
- [flow-collector on page 396](#)
- [flow-export-destination on page 397](#)
- [flow-export-rate on page 397](#)
- [flow-inactive-timeout on page 398](#)
- [flow-monitoring on page 399](#)
- [flow-server on page 400](#)
- [flow-table-size on page 401](#)
- [flow-tap on page 402](#)
- [ftp \(Flow Collector Files\) on page 403](#)
- [ftp \(Transfer Log Files\) on page 404](#)
- [g-duplicates-dropped-periodicity on page 404](#)
- [g-max-duplicates on page 405](#)
- [generate-snmp-traps on page 405](#)
- [hard-limit on page 406](#)
- [hard-limit-target on page 406](#)
- [hardware-timestamp on page 407](#)
- [history-size on page 407](#)
- [host-outbound on page 408](#)
- [in-service \(RFC2544 Benchmarking\) on page 409](#)
- [inactivity-timeout \(Services RPM\) on page 409](#)
- [inline-jflow on page 410](#)
- [input \(Port Mirroring\) on page 410](#)
- [input \(Sampling\) on page 411](#)
- [input-interface-index on page 411](#)
- [input-packet-rate-threshold on page 412](#)
- [instance \(Sampling\) on page 413](#)
- [interface \(Accounting or Sampling\) on page 414](#)
- [interfaces on page 415](#)
- [interface \(Services Flow Tap\) on page 415](#)

- [interface-map](#) on page 416
- [interfaces \(Services Dynamic Flow Capture\)](#) on page 416
- [interfaces \(Video Monitoring\)](#) on page 417
- [inet6-options \(Services\)](#) on page 418
- [ip-swap \(RFC 2544 Benchmarking\)](#) on page 418
- [ipv4-flow-table-size](#) on page 419
- [ipv4-template](#) on page 419
- [ipv6-flow-table-size](#) on page 420
- [ipv6-extended-attrib](#) on page 420
- [ipv6-template](#) on page 421
- [jflow-log \(Interfaces\)](#) on page 422
- [jflow-log \(Services\)](#) on page 423
- [label-position](#) on page 424
- [license-server](#) on page 425
- [local-dump](#) on page 426
- [logical-system](#) on page 426
- [match](#) on page 427
- [max-connection-duration](#) on page 427
- [max-duplicates](#) on page 428
- [max-packets-per-second](#) on page 429
- [maximum-age](#) on page 429
- [maximum-connections](#) on page 430
- [maximum-connections-per-client](#) on page 431
- [maximum-packet-length](#) on page 432
- [maximum-sessions](#) on page 433
- [maximum-sessions-per-connection](#) on page 434
- [media-loss-rate](#) on page 435
- [media-rate-variation](#) on page 436
- [message-rate-limit \(Flow Monitoring Logs for NAT\)](#) on page 437
- [minimum-priority](#) on page 438
- [mode \(RFC 2544 Benchmarking\)](#) on page 438
- [monitoring](#) on page 439
- [moving-average-size](#) on page 440
- [mpls-ipv4-template](#) on page 440
- [mpls-template](#) on page 441
- [multiservice-options](#) on page 441
- [name-format](#) on page 442

- [next-hop \(Forwarding Options\) on page 443](#)
- [next-hop-group \(Forwarding Options\) on page 444](#)
- [next-hop-group \(Port Mirroring\) on page 445](#)
- [no-filter-check on page 445](#)
- [no-remote-trace \(Trace Options\) on page 446](#)
- [no-syslog on page 446](#)
- [no-syslog-generation on page 447](#)
- [notification-targets on page 447](#)
- [observation-domain-id on page 448](#)
- [one-way-hardware-timestamp on page 449](#)
- [option-refresh-rate on page 450](#)
- [options-template-id on page 451](#)
- [output \(Accounting\) on page 452](#)
- [output \(Monitoring\) on page 453](#)
- [output \(Port Mirroring\) on page 454](#)
- [output \(Sampling\) on page 455](#)
- [output-interface-index on page 456](#)
- [passive-monitor-mode on page 456](#)
- [password \(Flow Collector File Servers\) on page 457](#)
- [password \(Transfer Log File Servers\) on page 457](#)
- [peer-as-billing-template on page 458](#)
- [pic-memory-threshold on page 458](#)
- [pop-all-labels on page 459](#)
- [port \(Flow Monitoring\) on page 460](#)
- [port \(RPM\) on page 460](#)
- [port \(TWAMP\) on page 461](#)
- [port-mirroring on page 462](#)
- [post-cli-implicit-firewall on page 463](#)
- [pre-rewrite-tos on page 464](#)
- [probe on page 465](#)
- [probe-count on page 466](#)
- [probe-interval on page 467](#)
- [probe-limit on page 467](#)
- [probe-server on page 468](#)
- [probe-type on page 469](#)
- [rate \(Forwarding Options\) on page 470](#)
- [receive-options-packets on page 471](#)

- [receive-ttl-exceeded](#) on page 471
- [refresh-rate](#) (Flow Monitoring Logs for NAT) on page 472
- [reflect-mode](#) (RFC2544 Benchmarking) on page 473
- [reflect-etype](#) (RFC 2544 Benchmarking) on page 474
- [required-depth](#) on page 475
- [retry](#) (Services Flow Collector) on page 476
- [retry-delay](#) on page 476
- [rfc2544-benchmarking](#) on page 477
- [routing-instance](#) on page 478
- [routing-instance \(cflowd\)](#) on page 479
- [routing-instance-list](#) (TWAMP) on page 480
- [routing-instances](#) on page 481
- [rpm](#) (Interfaces) on page 482
- [rpm](#) (Services) on page 483
- [run-length](#) on page 485
- [sample-once](#) on page 485
- [sampling](#) (Forwarding Options) on page 486
- [sampling](#) (Interfaces) on page 488
- [server](#) on page 489
- [server-inactivity-timeout](#) on page 489
- [service-port](#) on page 490
- [service-type](#) (RFC2544 Benchmarking) on page 490
- [services](#) on page 491
- [services](#) on page 491
- [services-options](#) on page 492
- [shared-key](#) on page 493
- [size](#) on page 493
- [soft-limit](#) on page 494
- [soft-limit-clear](#) on page 494
- [source-address](#) (Forwarding Options) on page 495
- [source-address](#) (Services) on page 496
- [source-addresses](#) on page 496
- [source-id](#) on page 497
- [source-ip](#) (Flow Monitoring Logs for NAT) on page 498
- [source-ipv4-address](#) (RFC 2544 Benchmarking) on page 499
- [source-mac-address](#) (RFC2544 Benchmarking) on page 499
- [source-udp-port](#) (RFC 2544 Benchmarking) on page 500



- [stamp](#) on page 500
- [storm-control](#) on page 501
- [syslog](#) on page 501
- [target \(Services RPM\)](#) on page 502
- [tcp](#) on page 503
- [templates](#) on page 504
- [test](#) on page 506
- [tests \(RFC 2544 Benchmarking\)](#) on page 507
- [test-interface \(RFC 2544 Benchmarking\)](#) on page 508
- [test-interval](#) on page 509
- [test-name \(RFC 2544 Benchmarking\)](#) on page 510
- [test-session](#) on page 511
- [thresholds](#) on page 512
- [traceoptions \(Dynamic Flow Capture\)](#) on page 513
- [traceoptions \(Forwarding Options\)](#) on page 514
- [traceoptions \(RPM\)](#) on page 515
- [transfer](#) on page 516
- [transfer-log-archive](#) on page 517
- [traps](#) on page 518
- [ttl](#) on page 519
- [twamp](#) on page 520
- [twamp-server](#) on page 521
- [template \(Forwarding Options\)](#) on page 521
- [template-id](#) on page 522
- [template-profile \(Flow Monitoring Logs for NAT\)](#) on page 523
- [template-refresh-rate](#) on page 524
- [template-type \(Flow Monitoring Logs for NAT\)](#) on page 525
- [trio-flow-offload](#) on page 526
- [udp](#) on page 526
- [udp-tcp-port-swap \(RFC 2544 Benchmarking\)](#) on page 527
- [unit](#) on page 528
- [username \(Services\)](#) on page 529
- [variant](#) on page 529
- [version](#) on page 530
- [version \(Flow Monitoring Logs for NAT\)](#) on page 531
- [version9 \(Forwarding Options\)](#) on page 531
- [version-ipfix \(Services\)](#) on page 532

- [video-monitoring](#) on page 533
- [world-readable](#) on page 534

## **[edit forwarding-options] Hierarchy Level**

---

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 Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices*. This section documents only the statements used in flow monitoring and accounting services.

- Related Documentation**
- [\[edit interfaces\] Hierarchy Level on page 331](#)
  - [\[edit services flow-monitoring\] Hierarchy Level on page 334](#)

## [edit interfaces] Hierarchy Level

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;
 }
}

```

- Related Documentation
- [\[edit forwarding-options\] Hierarchy Level on page 328](#)
  - [\[edit services flow-monitoring\] Hierarchy Level on page 334](#)

## [\[edit services dynamic-flow-control\] Hierarchy Level](#)

To configure dynamic flow capture, include the **dynamic-flow-capture** statement at the **[edit services]** hierarchy level:

```

[edit services]
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;
traceoptions{
 file filename <files number> <size size> <world-readable | non-world-readable>;
}
}

```

Related Documentation • [Configuring Junos Capture Vision on page 81](#)

## [edit services flow-collector] Hierarchy Level

To configure flow collection, include the **flow-collector** statement at the **[edit services]** hierarchy level:

```

[edit services]
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;
 }
}
}

```

- Related Documentation**
- [Configuring Flow Collection on page 36](#)
  - [Sending cflowd Records to Flow Collector Interfaces on page 46](#)
  - [Configuring Flow Collection Mode and Interfaces on Services PICs on page 46](#)

## [edit services flow-monitoring] Hierarchy Level

```
[edit]
services {
 flow-monitoring {
 version9 {
 template template-name {
 flow-active-timeout seconds;
 flow-inactive-timeout seconds;
 ipv4-template {
 nexthop-options {
 mpls {
 label-position [positions];
 }
 }
 }
 ipv6-template;
 mpls-template {
 label-position [positions];
 }
 mpls-ipv4-template {
 label-position [positions];
 }
 option-refresh-rate {
 packets packets;
 seconds seconds;
 }
 peer-as-billing-template;
 template-refresh-rate {
 packets packets;
 seconds seconds;
 }
 peer-as-billing-template;
 option-refresh-rate packets;
 template-refresh-rate packets;
 }
 }
 }
}
```

- Related Documentation**
- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)
  - [\[edit services\] Hierarchy Level](#)



## [edit services flow-tap] Hierarchy Level

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.

```
[edit services]
 flow-tap {
 interface interface-name;
 family inet | inet6;
 }
```

Other statements are configured at the **[edit interfaces]** and **[edit system]** hierarchy levels.

### Related Documentation

- [Junos Packet Vision Architecture on page 92](#)
- [Configuring Junos Packet Vision on page 93](#)
- [Configuring FlowTapLite on page 96](#)

## [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;
 inet6-options;
```

```

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);
 authentication-key-chain identifier {
 key-id identifier {
 secret password-string;
 }
 }
 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;
 routing-instance-list {
 instance-name {
 port number;
 }
 }
 server-inactivity-timeout minutes;
 }
}
rfc2544-benchmarking {

```

```

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);
 }
}

```



**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 207](#).

#### Related Documentation

- [Configuring BGP Neighbor Discovery Through RPM on page 211](#)
- [Configuring RPM Probes on page 201](#)
- [Configuring RPM Receiver Servers on page 206](#)
- [Limiting the Number of Concurrent RPM Probes on page 206](#)
- [Configuring RPM Timestamping on page 207](#)
- [Configuring TWAMP on page 210](#)
- [Enabling RPM for the Junos OS Extension-Provider Package on page 221](#)
- [Tracing RPM Operations on page 215](#)

## 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 number;
 engine-type number;
 source-address 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 115](#)

## address (Interfaces)

|                                 |                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>address address {<br/>    destination address;<br/>}</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 6</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 103</a></li> </ul> |

## address (Services Dynamic Flow Capture)

|                                 |                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>address address;</code>                                                                                                      |
| <b>Hierarchy Level</b>          | [edit services dynamic-flow-capture <code>capture-group client-name content-destination identifier</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>                  | <b>address</b> —IP address for the content destination.                                                                            |
| <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 82</a></li> </ul>                 |

## aggregate-export-interval

---

|                                 |                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>aggregate-export-interval <i>seconds</i>;</code>                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">accounting name output</a> ],<br>[edit forwarding-options <a href="#">sampling instance instance-name family</a> (inet   inet6   mpls) <a href="#">output</a> ],<br>[edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) <a href="#">output</a> ] |
| <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>                  | <i>seconds</i> —Duration.                                                                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 115</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>          | <p>[edit forwarding-options <a href="#">accounting output cflowd hostname</a>],<br/> [edit forwarding-options <a href="#">sampling instance instance-name family</a> (inet   inet6   mpls) <a href="#">output flow-server hostname</a>],<br/> [edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) <a href="#">output flow-server hostname</a>]</p>                                                                                                                                                                                                                                                                                                                                |
| <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 132</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## alarms

```
Syntax alarms {
 delay-factor {
 no-syslog-generation;
 generate-snmp-traps;
 storm-control {
 count number;
 interval number;
 }
 alarm-mode {
 mdi-records-count number;
 average;
 }
 }
 media-rate-variation {
 no-syslog-generation;
 generate-snmp-traps;
 storm-control {
 count number;
 interval number;
 }
 alarm-mode {
 mdi-records-count number;
 average;
 }
 }
 media-loss-rate {
 no-syslog-generation;
 generate-snmp-traps;
 storm-control {
 count number;
 interval number;
 }
 alarm-mode {
 immediate;
 }
 }
 }
```

**Hierarchy Level** [edit services]

**Release Information** Statement introduced in Junos OS Release 15.1.

**Description** Configure the alarm to monitor and report active alarms. SNMP is used to monitor alarms raised by the inline video monitoring feature. The alarms are monitored in the network management system either to troubleshoot the problem or to diagnose degradation in video quality.

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**
- [Inline Video Monitoring Overview on page 309](#)
  - [delay-factor on page 366](#)
  - [no-syslog-generation on page 447](#)
  - [generate-snmp-traps on page 405](#)
  - [storm-control on page 501](#)
  - [alarm-mode on page 343](#)
  - [media-rate-variation on page 436](#)
  - [media-loss-rate on page 435](#)

## alarm-mode

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | alarm-mode {<br>mdi-records-count <i>number</i> ;<br>average;<br>}                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit services]                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | If this statement is configured you can set the alarm as immediate or average mode. If immediate alarm is configured, an immediate trap is raised at the end of interval duration when the metric value exceeds the configured range. If average alarm is configured, a trap is generated based on average value for the specified number of interval duration. |
| <b>Default</b>                  | The default alarm mode is immediate mode.                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <p><b>mdi-records-count</b>—Media delivery index record count number for immediate alarm mode.</p> <p><b>average</b>—If the alarm-mode is average, the respective trap are generated for average values that are not within the configured 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>• <a href="#">Inline Video Monitoring Overview on page 309</a></li> <li>• <a href="#">alarms on page 342</a></li> </ul>                                                                                                                                                                                                  |

## allowed-destinations

---

|                                 |                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>allowed-destinations [ <i>destinations</i> ];</code>                                                                        |
| <b>Hierarchy Level</b>          | [edit services dynamic-flow-capture <code>capture-group</code> <i>client-name</i> <code>control-source</code> <i>identifier</i> ] |
| <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>destinations</i> —Allowed content destination name.                                                                            |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 83</a></li></ul>                       |

## 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.<br>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 37</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.<br>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 37</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 38</a></li> </ul>   |

## authentication-mode

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | authentication-mode (authenticated   encrypted   none);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm twamp server],<br>[edit services rpm twamp client control-connection <i>control-client-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.5.<br>Support at the [edit <b>services rpm twamp client control-connection <i>control-client-name</i></b> ] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <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 must set the value to <b>none</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>authenticated</b>—Authenticate all TWAMP packets.</p> <hr/> <p> <b>NOTE:</b> This mode is supported only on TWAMP servers.</p> <hr/> <p><b>encrypted</b>—Encrypt all TWAMP packets.</p> <hr/> <p> <b>NOTE:</b> This mode is supported only on TWAMP servers.</p> <hr/> <p><b>none</b>—Do not authenticate or encrypt packets.</p> <hr/> <p> <b>NOTE:</b> This mode is supported on both TWAMP servers and clients.</p> <hr/> |
| <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 TWAMP on page 210</a></li> <li>• <a href="#">Two-Way Active Measurement Protocol Overview on page 201</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## authentication-key-chain (TWAMP)


|                                 |                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>authentication-key-chain <i>identifier</i> {     key-id <i>identifier</i> {         secret <i>password-string</i>;     } }</pre>                                                                                                                                                                                                                                           |
| <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>              | <p>Apply and enable an authentication keychain to the routing device. Note that the referenced key chain must be defined. When configuring the authentication key update mechanism for TWAMP, you cannot commit the <b>0.0.0.0/allow</b> statement with authentication keys or key chains. The CLI issues a warning and fails to commit such configurations.</p>                |
| <b>Options</b>                  | <p><b><i>identifier</i></b>—Authentication keychain name. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (" ").</p> <p><b><i>password-string</i></b>—Authentication key, consisting of 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.</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 TWAMP on page 210</a></li> </ul>                                                                                                                                                                                                                                                                               |

## autonomous-system-type

---

|                                 |                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>autonomous-system-type (origin   peer);</code>                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit forwarding-options <b>sampling instance</b> <i>instance-name</i> <b>family</b> (inet   inet6   mpls) <b>output flow-server</b> <i>hostname</i> ],<br>[edit forwarding-options <b>sampling family</b> (inet   inet6   mpls) <b>output flow-server</b> <i>hostname</i> ] |
| <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>                  | <b>origin</b> —Export origin AS numbers of the packet source address in the Source Autonomous System cflowd field.<br><br><b>peer</b> —Export peer AS numbers through which the packet passed in the Source Autonomous System cflowd field.                                  |
| <b>Required Privilege Level</b> | <code>interface</code> —To view this statement in the configuration.<br><code>interface-control</code> —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 132</a></li></ul>                                                                                                                                                                      |

## bgp

|                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                            | <pre> bgp {   data-fill <i>data</i>;   data-size <i>size</i>;   destination-port <i>port</i>;   history-size <i>size</i>;   logical-system <i>logical-system-name</i> &lt;routing-instances <i>routing-instance-name</i>&gt;;   moving-average-size <i>size</i>;   probe-count <i>count</i>;   probe-interval <i>seconds</i>;   probe-type <i>type</i>;   routing-instances <i>instance-name</i>;   test-interval <i>interval</i>; } </pre>                                      |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                   | <pre> [edit <a href="#">services</a> rpm bgp], [edit protocols bgp group <i>group-name</i>], [edit <a href="#">routing-instances</a> <i>instance-name</i> protocols bgp group <i>group-name</i>], [edit <a href="#">logical-system</a> <i>logical-system-name</i> protocols bgp group <i>group-name</i>], [edit <a href="#">logical-system</a> <i>logical-system-name</i> <a href="#">routing-instances</a> <i>instance-name</i> protocols bgp   group <i>group-name</i>] </pre> |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                               | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>                                                                                                                                                                                                                                                                                                       | Configure BGP neighbor discovery through Real-Time Performance Monitoring (RPM).                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                                                                                                                                                                                                                                                                                                           | <p><b>bgp</b>—Define properties for configuring BGP neighbor discovery.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                            |
| <div>  <p><b>NOTE:</b> On MX Series routers, you can configure all the statements. On M Series and T Series routers, you can configure only the <code>logical-system</code> and <code>routing-instances</code> statements.</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 BGP Neighbor Discovery Through RPM on page 211</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                     |

## capture-group

---

**Syntax**    `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;  
                }`

**Hierarchy Level**    [edit services dynamic-flow-capture]

**Release Information**    Statement introduced in Junos OS Release 7.4.

**Description**    Define the capture group values.

**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 the Capture Group on page 81](#)



## cflowd (Discard Accounting)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> cflowd <i>hostname</i> {     aggregation {         autonomous-system;         destination-prefix;         protocol-port;         source-destination-prefix {             caida-compliant;         }         source-prefix;     }     autonomous-system-type (origin   peer);     label-position {         template <i>template-name</i>;     }     (local-dump   no-local-dump);     port <i>port-number</i>;     source-address <i>address</i>;     version <i>format</i>; } </pre> |
| <b>Hierarchy Level</b>          | [edit forwarding-options <b>accounting</b> <i>name</i> <b>output</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <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 one version 5 and one version 8 flow format at the [edit forwarding-options <b>accounting</b> <i>name</i> <b>output</b>] hierarchy level.</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 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="#">Enabling Flow Aggregation on page 132</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                  |

## cflowd (Flow Monitoring)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>cflowd hostname {<br/>    port port-number;<br/>}</code>                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit forwarding-options <b>monitoring name</b> inet <b>output</b> ]                                                                                                                                                                                                                                                                                               |
| <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 forwarding-options <b>monitoring name output</b>] 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>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 132</a></li></ul>                                                                                                                                                                                                                                                            |

## client

```
Syntax client {
 control-connection control-client- name {
 authentication-mode
 destination-interface interface-name;
 destination-port port;
 history-size size;
 moving-average-size number;
 routing-instance instance-name;
 target (url url | address address);
 test-interval interval;
 traps traps;
 data-fill-with zeros
 data-size size;
 dscp-code-point dscp-bits;
 probe-count count;
 probe-interval seconds;
 thresholds thresholds;
 test-session session-name{
 data-fill-with zeros data;
 data-size size;
 dscp-code-point dscp-bits;
 probe-count count;
 probe-interval seconds;
 target (url url | address address);
 }
 }
 }
```

**Hierarchy Level** [edit services rpm twamp]

**Release Information** Statement introduced in Junos OS Release 15.1.

**Description** Specify the TWAMP client configuration settings.

**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**

- [Two-Way Active Measurement Protocol Overview on page 201](#)

## client-list

---

|                                 |                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>client-list <i>list-name</i> {<br/>    address <i>address</i>;<br/>}</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.<br><br><i>address</i> —Address and mask for an allowed client.                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>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 210</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.<br>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 38</a></li></ul>             |

## collector (Flow Monitoring Logs for NAT)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>collector <i>collector-name</i> {     source-ip <i>address</i>;     destination-address <i>address</i>;     destination-port <i>port-number</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit services jflow-log]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <p>Specify the name of the collector to which flow monitoring log messages in IPFIX or version 9 flow template format for NAT events must be sent. The generated flow monitoring logs for NAT events in flow template format are sent to the specified host or external device that functions as the NetFlow collector. You must associate a collector with a template profile for the template characteristics, such as refresh rate of messages and the template format, to be used for generated flow monitoring logs.</p>                 |
| <b>Options</b>                  | <p><b><i>collector-name</i></b>—Name of the collector to which flow monitoring log messages for NAT events in flow monitoring format (IPFIX or version 9 flow template format) must be sent. The name can be up to 32 alphanumeric characters in length. Allowed characters are [a-zA-Z0-9_]</p> <p>The remaining statements 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="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li> <li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li> <li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li> <li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</a></li> </ul> |

## collector (Flow Template Profiles for NAT)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>collector <i>collector-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | <code>[edit services jflow-log template-profile <i>template-profile-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Specify the name of the collector to be associated with a template profile. The generated flow monitoring logs for NAT events in flow template format are sent to the specified collector. You must have previously configured the collector by using the <b>collector collector-name</b> statement at the <b>[edit services jflow-log]</b> hierarchy level before you associate a collector with a template profile.                                                                                                                    |
| <b>Options</b>                  | <b>collector-name</b> —Name of the collector to which flow monitoring log messages for NAT events in flow monitoring format (IPFIX or version 9 flow template format) must be sent. The name can be up to 32 alphanumeric characters in length. Allowed characters are [a-zA-Z0-9_]                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li><li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li><li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li><li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</a></li></ul> |

## collector-group (Flow Template Profiles for NAT)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>collector-group <i>collector-group-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | <code>[edit services jflow-log template-profile <i>template-profile-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Specify the name of the collector group to be associated with a template profile. The generated flow monitoring logs for NAT events in flow template format are sent to the specified collector group. By using a collector group, you can effectively and optimally transmit flow monitoring logs to a cluster of collectors in a single, one-step operation. A maximum of up to eight collectors can be aggregated into a collector group. You must have previously configured the collector group by using the <b>collector-group collector-group-name</b> statement at the <code>[edit services jflow-log]</code> hierarchy level before you associate a collector-group with a template profile. |
| <b>Options</b>                  | <b>collector-group-name</b> —Name of the collector group to which log messages for NAT events in flow monitoring format (IPFIX or version 9 flow template format) must be sent. The name can be up to 32 alphanumeric characters in length. Allowed characters are <code>[a-zA-Z0-9_]</code>                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li> <li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li> <li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li> <li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</a></li> </ul>                                                                                                                                                         |

## collector-group (Flow Monitoring Logs for NAT)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>collector-group <i>collector-group-name</i> {<br/>    [<i>collector-name1 collector-name2</i>];<br/>}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit services jflow-log]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <p>Specify the name of the collector group that contains a set of NetFlow collectors to which flow monitoring log messages in IPFIX or version 9 flow template format for NAT events must be sent. You must define at least one collector in the group. A maximum of up to eight collectors can be aggregated into a collector group.</p> <p>The generated flow monitoring logs for NAT events in flow template format are sent to the specified collector group. By using a collector group, you can effectively and optimally transmit flow monitoring logs to a cluster of collectors in a single, one-step operation.</p>                                                                                                                                                                                          |
| <b>Options</b>                  | <p><b><i>collector-group-name</i></b>—Name of the collector group to which flow monitoring log messages for NAT events in flow monitoring format (IPFIX or version 9 flow template format) must be sent. The name can be up to 32 alphanumeric characters in length. Allowed characters are [a-zA-Z0-9_]</p> <p><b><i>collector-name</i></b>—Name of the collector to be assigned to the group of collectors. You must have previously defined the collector by including the <b>collector <i>collector-name</i></b> statement at the [edit services jflow-log] hierarchy level. You can specify a list of valid collector names. Specify the names individually by using a space to separate each collector name. The name can be up to 32 alphanumeric characters in length. Allowed characters are [a-zA-Z0-9_]</p> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li><li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li><li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li><li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</a></li></ul>                                                                                                                                                                                                                                                                               |



## content-destination

---

|                                 |                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>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>; }</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 82</a></li> </ul>                                                                                                                         |

## control-connection

**Syntax** `control-connection control-client-name {  
     authentication-mode  
     destination-interface interface-name;  
     destination-port port;  
     history-size size;  
     moving-average-size number;  
     routing-instance instance-name;  
     target (url url | address address);  
     test-interval interval;  
     traps traps;  
     data-fill-with-zeros data;  
     data-size size;  
     dscp-code-point dscp-bits;  
     probe-count count;  
     probe-interval seconds;  
     thresholds thresholds;  
     test-session session-name {  
         data-fill-with-zeros data;  
         data-size size;  
         dscp-code-point dscp-bits;  
         probe-count count;  
         probe-interval seconds;  
         target (url url | address address);  
     }  
 }`

**Hierarchy Level** [edit services rpm twamp client]

**Release Information** Statement introduced in Junos OS Release 15.1.

**Description** List all the TWAMP control clients that can connect to this server. You must configure at least one client to enable TWAMP.

**Options** *control-client-name*—Name of the control client.

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**

- [Two-Way Active Measurement Protocol Overview on page 201](#)


## control-source

---

|                                 |                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <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> |
| <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 source of the dynamic flow capture request.                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><i>identifier</i>—Name of control source.</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 Control Source on page 83</a></li> </ul>                                                                                                                                                                                                       |

## core-dump

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | (core-dump   no-core-dump);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit <a href="#">interfaces</a> mo-fpc/pic/port <a href="#">multiservice-options</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | <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>                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 6</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## data-fill

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>data-fill data;</code><br><code>data-fill-with-zeros data;</code>                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit services rpm bgp],<br>[edit <a href="#">services (RPM)</a> rpm probe owner test test-name]                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 9.3 for PTX Series Packet Transport Routers.<br>Statement at the [edit services rpm twamp client control-connection control-client-name] hierarchy level introduced in Junos OS Release 15.1 for MX Series 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. For TWAMP client, if this knob is set, then fill the test packet with zeros, if the knob is not set then the data content would be random value as indicated in RFC.           |
| <b>Options</b>                  | <b>data</b> —A hexadecimal value; for example, <b>0-9</b> , <b>A-F</b> .                                                                                                                                                                                                                                                                                                                  |
| <b>Usage Guidelines</b>         | The <b>data-fill</b> statement is not valid with the <b>http-get</b> or <b>http-metadata-get</b> probe types. See <a href="#">“Configuring BGP Neighbor Discovery Through RPM” on page 211</a> or <i>Configuring Real-Time Performance Monitoring</i> .                                                                                                                                   |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>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 211</a></li> <li>• <a href="#">Configuring RPM Probes on page 201</a></li> </ul>                                                                                                                                                                                              |

## data-fill-with-zeros

---

|                                 |                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>data-fill-with-zeros;</code>                                                                                                                                                      |
| <b>Hierarchy Level</b>          | <code>[edit services rpm twamp client control-connection <i>control-client-name</i> test-session <i>session-name</i>]</code>                                                            |
| <b>Release Information</b>      | Statement at the <code>[edit services rpm twamp client control-connection <i>control-client-name</i>]</code> hierarchy level introduced in Junos OS Release 15.1 for MX Series routers. |
| <b>Description</b>              | If this statement is configured, then the contents of the test packet are zeros, if the statement is not configured, then the data content is a pseudo-random number.                   |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Two-Way Active Measurement Protocol Overview on page 201</a></li></ul>                                                              |

## data-format

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>data-format <i>format</i>;</code>                                                                                 |
| <b>Hierarchy Level</b>          | <code>[edit services flow-collector file-specification variant <i>variant-number</i>]</code>                            |
| <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.<br>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 37</a></li></ul>                   |

## data-size

|                            |                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>data-size size;</code>                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>     | [edit services rpm bgp],<br>[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> test-name],<br>[edit services rpm twamp client control-connection <i>control-client-name</i> test-session session-name]                                                                                                                                                          |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.<br>Support at the [edit services rpm twamp client control-connection <i>control-client-name</i> ] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers. |
| <b>Description</b>         | 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.                                                                                                                                                                                                                                |
| <b>Options</b>             | <b>size</b> —0 through 65400 for RPM, for TWAMP the value is from 60 through 1400.<br><b>Default:</b> 0 for RPM and 60 for TWAMP.                                                                                                                                                                                                                                                                |



**NOTE:** If you configure the hardware timestamp feature (see [“Configuring RPM Timestamping” on page 207](#)):

- The default value of **data-size** 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.

|                                 |                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>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 211</a></li> </ul> |

## delay-factor

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>delay-factor {<br/>    no-syslog-generation;<br/>    generate-snmp-traps;<br/>    storm-control {<br/>        count <i>number</i>;<br/>        interval <i>number</i>;<br/>    }<br/>    alarm-mode {<br/>        mdi-records-count <i>number</i>;<br/>        average;<br/>    }<br/>}</pre>                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit services]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | <p>Configure the maximum observed time difference between the arrival of media data and the drain of media data. The delay factor suggests the minimum size of the buffer required at the next downstream node. As a stream progresses, the variation of the delay factor indicates packet bunching or packet gaps (jitter). Greater delay factor values also indicate that more network latency is needed to deliver a stream because of the need to pre-fill a receive buffer before beginning the drain to guarantee no underflow.</p> <p>The remaining statements are explained separately.</p> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Inline Video Monitoring Overview on page 309</a></li><li>• <a href="#">alarms on page 342</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                         |



## destination (Interfaces)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>destination address;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | <p>[edit interfaces <i>interface-name</i> unit <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</a></li> <li>• <a href="#">Configuring Encryption Interfaces</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 103</a></li> <li>• <a href="#">Configuring Flow Monitoring on page 6</a></li> <li>• <a href="#">Configuring Unicast Tunnels</a></li> </ul> |

## destination-address (Flow Monitoring Logs for NAT)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>destination-address <i>address</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | <code>[edit services jflow-log collector <i>collector-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | Specify the destination IP address or identifier of the host or external device that functions as the collector for receiving the generated flow monitoring logs that are sent from the exporter. You can configure an IPv4 address, or an identifier of the host system (the workstation either running the Jflow utility or collecting traffic flows using version 9 or IPFIX format). For external NetFlow collectors or 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 a maximum of eight collectors per profile. |
| <b>Options</b>                  | <b><i>address</i></b> —Destination hostname, or IPv4 or IPv6 address of the collector.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li><li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li><li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li><li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</a></li></ul>                                                                                                            |

## destination-interface

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>destination-interface <i>interface-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit <b>services rpm probe owner test test-name</b> ],<br>[edit <b>services rpm probe-server (tcp   udp)</b> ],<br>[edit <b>services rpm twamp client control-connection control-client-name</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.5.<br>Support at the [edit <b>services rpm twamp client control-connection control-client-name</b> ] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | <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>The inline service interface (<b>si-</b> interface) is a virtual physical service interface that resides on the Packet Forwarding Engine to provide L2TP services without a special services PIC. The inline service interface is supported only by MPCs on MX Series routers. Four inline service interfaces are configurable per MPC-occupied chassis slot. Specify a multiservices (<b>si-</b>) interface that adds a timestamp to TWAMP probe messages. You must also configure the <b>rpm twamp-client</b> or <b>twamp-server</b> statement on the <b>si-</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> |
| <b>Options</b>                  | <b>interface-name</b> —Name of the adaptive services interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | <b>system</b> —To view this statement in the configuration.<br><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 Timestamping on page 207</a></li> <li>• <a href="#">Configuring RPM Receiver Servers on page 206</a></li> <li>• <a href="#">hardware-timestamp on page 407</a></li> <li>• <a href="#">rpm (Interfaces) on page 482</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

- [Enabling RPM for the Junos OS Extension-Provider Package on page 221](#)

---

## 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 rpm rfc2544-benchmarkingtests test-name test-name</a> ]                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3X52 for ACX Series routers.<br>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.<br><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.<br><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 235</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">rfc2544-benchmarking on page 477</a></li></ul> |

## destination-mac-address (RFC2544 Benchmarking)

|                                 |                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>destination-mac-address <i>mac-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 12.3X53 for ACX Series routers.<br>Statement introduced in Junos OS Release 14.2 for MX104 3D Universal Edge Routers.                                                                                                               |
| <b>Description</b>              | Specify the destination MAC address used in the generated test frames. This is a mandatory parameter for family <b>bridge</b> .                                                                                                                                              |
| <b>Options</b>                  | <b><i>mac-address</i></b> —MAC address. Specify the MAC address as six hexadecimal bytes in one of the following formats: <i>nnnn.nnnn.nnnn</i> or <i>nn:nn:nn:nn:nn:nn</i> —for example, <b>0011.2233.4455</b> or <b>00:11:22:33:44:55</b> .                                |
| <b>Required Privilege Level</b> | <b>interface</b> —To view this statement in the configuration.<br><b>interface-control</b> —To add this statement to the configuration.                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">rfc2544-benchmarking on page 477</a></li> <li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li> <li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li> </ul> |

## destination-port

|                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                          | <code>destination-port <i>port</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>                                                                                                                                                 | <code>[edit services rpm bgp],</code><br><code>[edit <b>services</b> rpm <b>probe</b> owner <b>test</b> <i>test-name</i>],</code><br><code>[edit services rpm twamp client control-connection <i>control-client-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                       |
| <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> <p>Support at the <code>[edit <b>services</b> rpm twamp client control-connection <i>control-client-name</i>]</code> hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.</p>                                                                                                                                                                                                 |
| <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 the destination port 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>                                                                                                                                                         | <p><b>Default:</b> The default value for the port is 862 to which the TWAMP client establishes control connection.</p> <p><b>port</b>—The port number can be 7 or from 49,160 through 65,535.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <div>  <b>NOTE:</b> The specified port numbers are recommended for RPM only. </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b>                                                                                                                                        | <p>system—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 BGP Neighbor Discovery Through RPM on page 211</a></li> <li>• <a href="#">Configuring RPM Probes on page 201</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## destination-port (Flow Monitoring Logs for NAT)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>destination-port <i>port-number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | <code>[edit services jflow-log collector <i>collector-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Specify the UDP port of the destination to be used in the UDP header for the generated flow monitoring logs. This is a required setting.                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <p><i>port-number</i>—UDP port number for the test frames.</p> <p><b>Default:</b> 4041</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="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li> <li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li> <li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li> <li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</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>          | <code>[edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> <i>test-name</i> <i>test-name</i>]</code>                                                                                                                                                 |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 12.3X52 for ACX Series routers.</p> <p>Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.</p>                                                                                                    |
| <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>                  | <p><i>port-number</i>—UDP port number for the test frames</p> <p><b>Default:</b> 4041</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 235</a></li> <li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li> <li>• <a href="#">rfc2544-benchmarking on page 477</a></li> </ul> |

## destinations

---

|                                 |                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>destinations {<br/>  ftp:url {<br/>    password "password";<br/>  }<br/>}</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.<br>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 36</a></li></ul> |



## direction (RFC2544 Benchmarking)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | direction (egress   ingress);                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> test-name test-name]                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3X52 for ACX Series routers.<br>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 and a <b>bridge</b> family. RFC2544 tests are supported only in the egress direction or the user-to-network interface (UNI) direction of an E-line or E-LAN service parameters in a bridge domain between two routers for unicast traffic. You cannot compute the NNI direction of Ethernet services between two routers for multicast or broadcast traffic. |
| <b>Options</b>                  | <p><b>egress</b>—Run the test in the egress direction of the interface (network-to-network interface (NNI)). This option is applicable for a <b>ccc</b> and <b>bridge</b> family.</p> <p><b>ingress</b>—Run the test in the ingress direction of the interface (user-to-network interface (UNI)). You cannot configure this option for a <b>bridge</b> family.</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="#">rfc2544-benchmarking on page 477</a></li> <li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li> <li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li> </ul>                                                                                                                                                                                                            |

## disable (Forwarding Options)

---

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax              | disable;                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Hierarchy Level     | [edit forwarding-options port-mirror],<br>[edit forwarding-options port-mirror instance <i>instance-name</i> ],<br>[edit forwarding-options <a href="#">sampling</a> ],<br>[edit forwarding-options <a href="#">sampling instance</a> <i>instance-name</i> ],<br>[edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) ],<br>[edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) <a href="#">output file</a> ] |
| Release Information | Statement introduced before Junos OS Release 7.4.<br>Statement added to <b>port-mirror</b> hierarchy in Junos OS Release 9.6.                                                                                                                                                                                                                                                                                                                                      |



**NOTE:** Beginning in Junos OS 15.1F5 and later 15.1 releases, the **disable** option has been deprecated at the forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls) hierarchy level on PTX3000 routers. When configured, the option does not take effect, so packets continue to be sampled. Instead of the **disable** option, use the **deactivate forwarding-options sampling instance *instance-name* family (inet | inet6 | mpls)** command to prevent sampling.

---

|                          |                                                                                                                                                                             |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description              | Disable traffic accounting, port mirroring, or sampling.                                                                                                                    |
| Required Privilege Level | interface—To view this statement in the configuration.<br>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 103</a></li><li>• <a href="#">Configuring Port Mirroring on page 173</a></li></ul> |

## disable-signature-check (RFC 2544 Benchmarking)

|                                 |                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | disable-signature-check;                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> test-name <i>test-name</i> ]                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3X53 for ACX Series routers.<br>Statement introduced in Junos OS Release 15.1 for MX104 3D Universal Edge routers.                                                                                                                                                           |
| <b>Description</b>              | Disable signature verification on the received test frames. This statement is valid only if you configure the test mode to be a reflector. The configuration is useful when the test traffic is generated using a third-party vendor tool, instead of an ACX Series router.                                              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li> <li>• <a href="#">Supported RFC2544-Based Benchmarking Statements on MX104 Routers on page 234</a></li> <li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</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> ],<br>[edit services rpm twamp client control-connection <i>control-client-name</i> test-session <i>session-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release for PTX Series Packet Transport Routers.<br>Support at the [edit services rpm twamp client control-connection <i>control-client-name</i> ] hierarchy level introduced in Junos OS Release 15.1 for MX Series 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>             | <i>dscp-bits</i> —A valid 6-bit pattern; for example, 001111, or one of the following configured DSCP aliases: <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></ul> |

- **ef**—Default: 101110
- **nc1**—Default: 110000
- **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 201](#)
- [Two-Way Active Measurement Protocol Overview on page 201](#)

## **duplicates-dropped-periodicity**

**Syntax** `duplicates-dropped-periodicity seconds;`

**Hierarchy Level** [edit services dynamic-flow-capture **capture-group** *client-name*]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify the frequency for sending notifications to affected control sources when transmission of duplicate sets of data is restricted because the **max-duplicates** threshold has been reached.

**Options** ***seconds***—Period for sending DuplicatesDropped notifications.  
**Default:** 30 seconds

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [g-duplicates-dropped-periodicity on page 404](#)
- [Limiting the Number of Duplicates of a Packet on page 87](#)
- [max-duplicates on page 428](#)

## dynamic-flow-capture


|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>dynamic-flow-capture {   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>;   }   g-duplicates-dropped-periodicity <i>seconds</i>;   g-max-duplicates <i>number</i>; }</pre> |
| <b>Hierarchy Level</b>          | [edit services]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Define the dynamic flow capture properties 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.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Junos Capture Vision</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## engine-id (Forwarding Options)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>engine-id <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <code>[edit forwarding-options <a href="#">accounting name</a> <a href="#">output interface</a> <i>interface-name</i>],</code><br><code>[edit forwarding-options <a href="#">monitoring name</a> <a href="#">output interface</a> <i>interface-name</i>],</code><br><code>[edit forwarding-options <a href="#">sampling instance</a> <i>instance-name</i> <a href="#">family</a> (inet   inet6   mpls) <a href="#">output</a></code><br><code><a href="#">interface</a> <i>interface-name</i>],</code><br><code>[edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) <a href="#">output interface</a> <i>interface-name</i>]</code> |
| <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 Level</b> | interface—To view this statement in the configuration.<br>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 103</a></li> <li>• <a href="#">Configuring Flow Monitoring on page 6</a></li> <li>• <a href="#">Configuring Discard Accounting on page 115</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                           |

## engine-type

---

|                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                                                                                                                                                                                                                                                                                                                                                                             | engine-type <i>number</i> ;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Hierarchy Level                                                                                                                                                                                                                                                                                                                                                                    | [edit forwarding-options <a href="#">accounting name</a> <a href="#">output interface interface-name</a> ],<br>[edit forwarding-options <a href="#">monitoring name</a> <a href="#">output interface interface-name</a> ],<br>[edit forwarding-options <a href="#">sampling instance instance-name family</a> (inet   inet6   mpls) <a href="#">output interface interface-name</a> ],<br>[edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) <a href="#">output interface interface-name</a> ] |
| Release Information                                                                                                                                                                                                                                                                                                                                                                | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Description                                                                                                                                                                                                                                                                                                                                                                        | <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> <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.</div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Options                                                                                                                                                                                                                                                                                                                                                                            | <i>number</i> —Platform-specific accounting interface type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Required Privilege Level                                                                                                                                                                                                                                                                                                                                                           | interface—To view this statement in the configuration.<br>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 103</a></li><li>• <a href="#">Configuring Flow Monitoring on page 6</a></li><li>• <a href="#">Configuring Discard Accounting on page 115</a></li></ul>                                                                                                                                                                                                                                                                            |



---

## export-format

---

|                                 |                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>export-format <i>format</i>;</code>                                                                                                 |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">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.<br><b>Values:</b> 5 or 8<br><b>Default:</b> 5                                                         |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 530</a></li><li>• <a href="#">Exporting Flows on page 9</a></li></ul> |

## extension-service

**Syntax**

```
extension-service
 service-name {
 provider-specific rules;
 }
 application {
 argument argument-names
 max-datasize datasize
 checksum
 daemonize
 }
 max-datasize datasize
 traceoptions {
 file filename
 flag flag
 no-remote-trace
 }
}
```

**Hierarchy Level** [edit forwarding-options **sampling instance** *instance-name* **family** (inet |inet6) **output**],  
[edit forwarding-options **sampling family** (inet |inet6) **output**],  
[edit services service-set *service-set-name*]  
set system services

**Release Information** Statement introduced in Junos OS Release 9.0.

**Description** Define a customer specific sampling configuration.

Define a service set or traffic monitoring for applications using application-specific configuration guidelines.



**NOTE:** If the **extension-service** statement is specified while configuring a service set, the **service-order** statement is mandatory.

Define configuration parameters for an application.

**Options** **provider-specific rules**—Provider-specific subhierarchy for services and service sets. See the application-specific documentation for details.

**service-name**—Name of the service.

**file script-name**—Name of the local script file.

**arguments argument-name**—Command line arguments to the JET application

**checksum number**—Checksum of the script.

**max-datasize datasize**—Maximum data segment size allowed for application execution (23068672..1073741824 bytes).

**daemonize**—Application runs as a background process.

**file *filename***—Name of the file to receive the output of the tracing operation. All files are placed in the directory /var/log.

**flag *flag***—Tracing operation to perform:

- **all**—Trace everything.
- **config**—Trace configuration events.
- **general**—Trace general events.
- **notification**—Trace notification events.
- **routing-socket**—Trace routing socket calls.
- **thriftv**—Trace thrift server events.
- **timeouts**—Trace timeouts.
- **timer**—Trace internal timer events.

**no-remote-trace**—Disable remote tracing.

|                                 |                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | <b>system</b> —To view this statement in the configuration.<br><b>system-control</b> —To add this statement to the configuration. |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|

|                              |                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <b>service-order</b></li><li>• <a href="#">sampling on page 486</a></li></ul> |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------|

## family (Monitoring)

---

**Syntax**

```
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;
 }
}
```

**Hierarchy Level** [edit forwarding-options [monitoring name](#)]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Specify input and output interfaces and properties for flow monitoring. Only IPv4 ([inet](#)) is supported.

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 6](#)

---

## 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.

**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 173](#)

## family (RFC2544 Benchmarking)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | family (bridge   ccc   inet);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> test-name test-name]                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3X52 for ACX Series routers.<br>Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.<br><b>bridge</b> option introduced in Junos OS Release 12.3X53 for ACX Series routers.<br><b>bridge</b> option introduced in Junos OS Release 14.2 for MX104 3D Universal Edge Routers.                                                                                                                                                                                                       |
| <b>Description</b>              | Configure the address type family for the benchmarking test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <p><b>bridge</b>—Indicates that the test is run on a Layer 2 Ethernet line (E- Line) or an Ethernet LAN (E-LAN) service configured in a bridge domain. You can run the RFC2544-based benchmarking test only in the egress direction or the user-to-network interface (UNI) direction of an Ethernet line.</p> <p><b>ccc</b>—Run the test on a circuit cross-connect (CCC) or Ethernet pseudowire service. You can run the RFC2544-based benchmarking test either in the egress or ingress direction.</p> <p><b>inet</b>—Run the test on an IPv4 service.</p> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">rfc2544-benchmarking on page 477</a></li><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li></ul>                                                                                                                                                                                                                                                                                     |

## family (Sampling)

**Syntax**

```
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;
 }
 }
}
```

**Hierarchy Level** [edit forwarding-options [sampling](#)],  
[edit forwarding-options [sampling instance](#) *instance-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.  
**mpls** option introduced in Release 8.3.  
**inet6** option introduced in Release 9.4.

**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 103](#)

---

## 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 103](#)



## file (Trace Options)

|                                 |                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | file <i>filename</i> <files <i>number</i> <size <i>bytes</i> > <world-readable   no-world-readable>;                                                                         |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">port-mirroring traceoptions</a> ],<br>[edit forwarding-options <a href="#">sampling traceoptions</a> ]                                  |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                            |
| <b>Description</b>              | Configure information about the files that contain trace logging information.                                                                                                |
| <b>Options</b>                  | <b><i>filename</i></b> —The name of the file containing the trace information.<br><b>Default:</b> /var/log/sampled<br><br>The remaining statements are explained separately. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 110</a></li> </ul>                                                          |

## file-specification (File Format)

|                                 |                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | file-specification {<br>variant <i>variant-number</i> {<br>data-format <i>format</i> ;<br>name-format <i>format</i> ;<br>transfer {<br>record-level <i>number</i> ;<br>timeout <i>seconds</i> ;<br>}<br>}<br>} |
| <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.<br>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 37</a></li> </ul>                                                                                                        |

## file-specification (Interface Mapping)

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | file-specification {<br>variant <i>variant-number</i> ;<br>}                                                            |
| <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.<br>interface-control—To add this statement to the configuration. |

## filename

---

|                                 |                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | filename <i>filename</i> ;                                                                                                             |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">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>              | Configure the name of the output file.                                                                                                 |
| <b>Options</b>                  | <i>filename</i> —Name of the file in which to place the traffic samples. All files are placed in the directory <code>/var/tmp</code> . |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 103</a></li></ul>                             |

## filename-prefix

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>filename-prefix <i>prefix</i>;</code>                                                                             |
| <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.<br>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 38</a></li> </ul>                |

## files

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>files <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">port-mirroring traceoptions file</a> ],<br>[edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) <a href="#">output file</a> ],<br>[edit forwarding-options <a href="#">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><i>number</i>—Maximum number of traffic sampling or trace log files. When a file named <i>sampling-file</i> reaches its maximum size, it is renamed <i>sampling-file.0</i>, then <i>sampling-file.1</i>, 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> | interface—To view this statement in the configuration.<br>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 173</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 103</a></li> </ul>                                                                                                                                                                                                                                                                                          |

## filter

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>filter {<br/>    input <i>filter-name</i>;<br/>    output <i>filter-name</i>;<br/>    group <i>filter-group-number</i>;<br/>}</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.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Routing Policies, Firewall Filters, and Traffic Policers 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 6</a></li></ul>                                                                                          |

## flow-active-timeout

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>flow-active-timeout <i>seconds</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>     | <code>[edit forwarding-options <b>accounting</b> <i>name</i> <b>output</b>],</code><br><code>[edit forwarding-options <b>monitoring</b> <i>name</i> <b>output</b>],</code><br><code>[edit forwarding-options <b>sampling</b> <i>instance</i> <i>instance-name</i> <b>family</b> (inet   inet6   mpls) <b>output</b>],</code><br><code>[edit forwarding-options <b>sampling</b> <b>family</b> (inet   inet6   mpls) <b>output</b>],</code><br><code>[edit <b>services</b> <b>flow-monitoring</b> <b>version</b> 9],</code><br><code>[edit <b>services</b> <b>flow-monitoring</b> <b>version-ipfix</b> <b>template</b> <i>template-name</i>]</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 <i>template-name</i>]</code> hierarchy level added in Junos OS Release 10.2.</p>                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>         | Set the interval after which an active flow is exported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



**NOTE:** The router must include an Adaptive Services, Multiservices, or Monitoring Services PIC for this statement to take effect.

|                |                                                                                                                                                                                                                                                                                                                                                           |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b> | <p><b><i>seconds</i></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> |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



**NOTE:** 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.

|                                 |                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <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 9</a></li> <li>• <a href="#">Configuring the Version 9 Template Properties on page 138</a></li> </ul> |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 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](#)

## flow-export-destination

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | flow-export-destination {<br>(cflowd-collector   collector-pic);<br>}                                                   |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">monitoring</a> <i>group-name</i> 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>                  | <b>cflowd-collector</b> —cflowd collector.<br><br><b>collector-pic</b> —Collector PIC.                                  |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | • <a href="#">Exporting Flows on page 9</a>                                                                             |


## flow-export-rate

---

|                                 |                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | flow-export-rate <i>rate</i> ;                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">sampling instance</a> <i>instance-name</i> family inet <a href="#">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>                  | <b>rate</b> —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.<br>interface-control—To add this statement to the configuration.                                                               |
| <b>Related Documentation</b>    | • <a href="#">Configuring Discard Accounting on page 115</a><br>• <a href="#">Configuring Flow Monitoring on page 6</a><br>• <a href="#">Configuring Traffic Sampling on page 103</a> |

## flow-inactive-timeout

---

|                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                        | <code>flow-inactive-timeout <i>seconds</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>                                                                                                                                                                                                               | <code>[edit forwarding-options <a href="#">accounting name output</a>],</code><br><code>[edit forwarding-options <a href="#">monitoring name output</a>],</code><br><code>[edit forwarding-options <a href="#">sampling instance instance-name family</a> (inet   inet6   mpls) <a href="#">output</a>],</code><br><code>[edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) <a href="#">output</a>],</code><br><code>[edit <a href="#">services flow-monitoring version9</a>],</code><br><code>[edit <a href="#">services flow-monitoringversion-ipfix template template-name</a>]</code> |
| <b>Release Information</b>                                                                                                                                                                                                           | Statement introduced before Junos OS Release 7.4.<br>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.<br><b>Range:</b> 60 through 1800 seconds (for <b>forwarding-options</b> configurations); 10 through 600 seconds (for <b>services</b> configurations)<br><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.<br><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 9</a></li><li>• <a href="#">Configuring the Version 9 Template Properties on page 138</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.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Flow Aggregation to Use Version 9 Flow Templates on page 137](#)

## flow-server

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <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>                                                                                               |
| <b>Hierarchy Level</b>     | [edit forwarding-options <b>sampling instance</b> <i>instance-name</i> <b>family</b> (inet   inet6   mpls) <b>output</b> ],<br>[edit forwarding-options <b>sampling family</b> (inet   inet6   mpls) <b>output</b> ]                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br><b>version9</b> statement introduced in Junos OS Release 8.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <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. 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 <b>[edit forwarding-options sampling family (inet   inet6   mpls) output flow-server <i>hostname</i>]</b> 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> |
| <b>Options</b>             | <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.

**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 103](#)

---

## flow-table-size

---

**Syntax**

```
flow-table-size {
 ipv4-flow-table-size units;
 ipv6-flow-table-size units;
 ipv6-extended-attrib;
}
```

**Hierarchy Level** [edit chassis fpc *slot-number* inline-services]

**Release Information** Statement introduced in Junos OS Release 12.1.  
**ipv6-extended-attrib** option added in Junos OS Release 14.2 for MX Series routers.

**Description** Configure the size of hash tables for inline services sampling.

**Options** The remaining statements are defined separately.

## flow-tap

---

|                                 |                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>flow-tap {<br/>  (<b>interface</b> <i>interface-name</i>   tunnel-interface <i>interface-name</i>   family (inet   inet6));<br/>}</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 93</a></li></ul>                                                                                                                   |

## 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 <b>collector interface-name</b> 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 <b>collector</b> 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> </ul> |

- **{year\_abbrev}**—From 00 through 99

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Destination FTP Servers for Flow Records on page 36](#)

---

## 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 Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Transfer Logs on page 38](#)

---

## g-duplicates-dropped-periodicity

---

**Syntax** `g-duplicates-dropped-periodicity seconds;`

**Hierarchy Level** [edit services dynamic-flow-capture]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify the frequency for sending notifications to affected control sources when transmission of duplicate sets of data is restricted because the **g-max-duplicates** threshold has been reached. This setting is applied globally; the **duplicates-dropped-periodicity** setting applied at the **capture-group** level overrides the global setting.

**Default** The default period for sending notifications is 30 seconds.

**Options** *seconds*—Period for sending DuplicatesDropped notifications.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.


**Related Documentation**

- [duplicates-dropped-periodicity on page 379](#)
- [Limiting the Number of Duplicates of a Packet on page 87](#)

## g-max-duplicates

|                                 |                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>g-max-duplicates <i>number</i>;</code>                                                                                                                                                                                                                                                                                      |
| <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 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. |
| <b>Default</b>                  | If no value is configured, a default setting of 3 is used.                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <i>number</i> —Maximum number of content destinations.<br><b>Range:</b> 1 through 64                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">max-duplicates on page 428</a></li> <li>• <a href="#">Limiting the Number of Duplicates of a Packet on page 87</a></li> </ul>                                                                                                                                                |

## generate-snmp-traps

|                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                  | <code>generate-snmp-traps;</code>                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                         | [edit services]                                                                                                                                                                                                                                           |
| <b>Release Information</b>                                                                                                                                                                                                                                                     | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                            |
| <b>Description</b>                                                                                                                                                                                                                                                             | If this statement is configured, the service generates SNMP traps for severity levels such as Info, Warning, Critical, or Cleared. For example, if DF alarm changes from info to warning, or from warning to critical, mdiDFAlarm trap will be triggered. |
| <div style="display: flex; align-items: center;">  <div> <p><b>NOTE:</b> SNMP traps are not generated if SNMP trap generation is not enabled.</p> </div> </div> |                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                   |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• <a href="#">Inline Video Monitoring Overview on page 309</a></li> <li>• <a href="#">alarms on page 342</a></li> </ul>                                                                                            |

## hard-limit

---

|                                 |                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>hard-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 the dynamic flow capture application begins deleting criteria, until the bandwidth falls below the <b>hard-limit-target</b> value. |
| <b>Options</b>                  | <b><i>bandwidth</i></b> —Hard limit threshold, in bits per second.                                                                                                        |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">hard-limit-target on page 406</a></li><li>• <a href="#">Configuring the Content Destination on page 82</a></li></ul>  |

## hard-limit-target

---

|                                 |                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>hard-limit-target <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 dynamic flow capture application stops deleting criteria.                                                              |
| <b>Options</b>                  | <b><i>bandwidth</i></b> —Target value, in bits per second.                                                                                                        |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 406</a></li><li>• <a href="#">Configuring the Content Destination on page 82</a></li></ul> |



## hardware-timestamp

|                                 |                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>hardware-timestamp;</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 in Junos OS Release 8.1.<br>Statement applied to MX Series routers in Junos OS Release 10.0.<br>Statement introduced in Junos OS Release 10.3 for EX Series switches.                                                 |
| <b>Description</b>              | 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. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                    |

## history-size

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>history-size <i>size</i>;</code>                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <code>[edit services rpm bgp],</code><br><code>[edit <b>services</b> rpm <b>probe</b> <i>owner</i> <b>test</b> <i>test-name</i>]</code><br><code>[edit services rpm twamp client control-connection <i>control-client-name</i>]</code>                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.<br>Statement at the <code>[edit services rpm twamp client control-connection <i>control-client-name</i>]</code> hierarchy level introduced in Junos OS Release 15.1 for MX Series routers. |
| <b>Description</b>              | Specify the number of stored history entries.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>                  | <b>size</b> —A value from 0 to 255.<br><b>Default:</b> 50                                                                                                                                                                                                                                                                                                                                                      |
| <b>Usage Guidelines</b>         | See “ <a href="#">Configuring BGP Neighbor Discovery Through RPM</a> ” on page 211 or <i>Configuring RPM Probes</i> .                                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 211</a></li> <li>• <a href="#">Configuring RPM Probes on page 201</a></li> </ul>                                                                                                                                                                                                                   |

## host-outbound

---

|                                 |                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | host-outbound media-interface;                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit chassis]                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2 on MX Series 3D Universal Edge Routers.                                                                                                                                                                   |
| <b>Description</b>              | <p>Enable Layer 2 port mirroring of host-generated outbound packets only on MPCs on MX Series 3D Universal Edge routers.</p> <p>This statement enables all Routing Engine-generated Layer 2 injections to execute egress logical interface filters.</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>Examples: Layer 2 Port Mirroring at Multiple Levels of the Chassis</i></li><li>• <i>Configuring Port Mirroring</i></li><li>• <i>Understanding Layer 2 Port Mirroring</i></li></ul>                           |

## in-service (RFC2544 Benchmarking)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>in-service;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <code>[edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> <i>test-name</i> <i>test-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3X53 for ACX Series routers.<br>Statement introduced in Junos OS Release 14.2 for MX104 3D Universal Edge Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | <p>Runs the test in the <b>in-service</b> mode. In this mode, while the test is running, the rest of the data traffic sent to and from the UNI port under test on the service are not interrupted. Control protocol packets and control protocol peering are not interrupted.</p> <p>If this mode is not configured, the test runs in the default <b>out-of-service</b> mode. In the <b>out-of-service</b> mode, while the test is running, all the data traffic sent to and from the UNI port under test on the service is interrupted. Control protocol peering is not interrupted whereas control protocol packets such as CFM sessions are interrupted.</p> |
| <b>Default</b>                  | The default service mode for the reflecting egress interface for an E-LAN service is <b>out-of-service</b> mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <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="#">rfc2544-benchmarking on page 477</a></li> <li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li> <li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                    |

## inactivity-timeout (Services RPM)

|                                 |                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>inactivity-timeout <i>seconds</i>;</code>                                                                                 |
| <b>Hierarchy Level</b>          | <code>[edit <a href="#">services</a> rpm twamp <a href="#">server</a>]</code>                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.3.                                                                                   |
| <b>Description</b>              | Inactivity timeout period, in seconds.                                                                                          |
| <b>Options</b>                  | <p><b><i>seconds</i></b>—Length of time the session is inactive before it times out.</p> <p><b>Default:</b> 1800 seconds</p>    |
| <b>Required Privilege Level</b> | <p>system—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 TWAMP on page 210</a></li> </ul>                               |

## inline-jflow

---

|                                 |                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>inline-jflow {<br/>    source-address <i>address</i>;<br/>    flow-export-rate <i>rate</i>;<br/>}</pre>                         |
| <b>Hierarchy Level</b>          | [edit forwarding-options <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.<br>Statement introduced in Junos OS Release 14.2 for T4000 routers with Type 5 FPC.   |
| <b>Description</b>              | Specify inline flow monitoring for traffic from the designated address.<br><br>The statements are explained separately.              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Inline Active flow Monitoring on page 122</a></li></ul>              |

## input (Port Mirroring)

---

|                                 |                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>input {<br/>    maximum-packet-length <i>bytes</i><br/>    rate <i>number</i>;<br/>    run-length <i>number</i>;<br/>}</pre>                                                                                                       |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">port-mirroring</a> ],<br>[edit forwarding-options <a href="#">port-mirroring</a> instance <i>instance-name</i> ]<br>[edit forwarding-options <a href="#">port-mirroring</a> family (inet   inet6)] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                       |
| <b>Description</b>              | Configure port mirroring on a logical interface.<br><br>The statements are explained separately.                                                                                                                                        |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 173</a></li></ul>                                                                                                                                |

## input (Sampling)

---

|                                 |                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | input {<br>max-packets-per-second <i>number</i> ;<br>rate <i>number</i> ;<br>run-length <i>number</i> ;<br>maximum-packet-length <i>bytes</i> ;<br>} |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">sampling</a> ],<br>[edit forwarding-options <a href="#">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.<br><br>The statements are explained separately.                                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 103</a></li> </ul>                                         |

## input-interface-index

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | input-interface-index <i>number</i> ;                                                                                   |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">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.<br>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 6</a></li> </ul>               |

## input-packet-rate-threshold

---

|                              |                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                | <code>input-packet-rate-threshold <i>rate</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 packet rate threshold value that triggers a system log warning message.                   |
| <b>Options</b>               | <i>rate</i> —Threshold value.                                                                       |
| <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 Thresholds on page 86</a></li></ul> |

## 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 Level</b> | interface—To view this statement in the configuration.<br>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 114</a></li></ul>           |

---

## interface (Accounting or Sampling)

---

|                                 |                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interface <i>interface-name</i> {<br/>    <i>engine-id</i> <i>number</i>;<br/>    <i>engine-type</i> <i>number</i>;<br/>    <i>source-address</i> <i>address</i>;<br/>}</pre>                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit forwarding-options <i>accounting</i> <i>name</i> <i>output</i> ],<br>[edit forwarding-options <i>sampling</i> <i>family</i> (inet   inet6   mpls) <i>output</i> ],<br>[edit forwarding-options <i>sampling</i> <i>instance</i> <i>instance-name</i> <i>family</i> (inet   inet6   mpls) <i>output</i> ] |
| <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>                  | <i>interface-name</i> —Name of the interface.<br><br>The remaining statements are explained separately.                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 115</a></li><li>• <a href="#">Configuring Traffic Sampling on page 103</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.<br>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>      |

## interface (Services Flow Tap)

---

|                                 |                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interface sp-<i>fpc/pic/port</i>.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>                  | <p><i>interface-name</i>—Name of the DFC interface.</p> <p>You cannot configure flow-tap services on channelized interfaces.</p>                                          |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 93</a></li> </ul>                                              |

## interface-map

---

|                                 |                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interface-map {<br/>    collector <i>interface-name</i>;<br/>    file-specification <i>variant-number</i>;<br/>    <i>interface-name</i> {<br/>        collector <i>interface-name</i>;<br/>        file-specification <i>variant-number</i>;<br/>    }<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit services flow-collector]                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                        |
| <b>Description</b>              | Match an input interface with a flow collector interface and apply the preset file specifications to the input interface.                                                                                                                                                |
| <b>Options</b>                  | The statements are explained separately.                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 38</a></li></ul>                                                                                                                                                              |

## interfaces (Services Dynamic Flow Capture)

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interfaces <i>interface-name</i>;</pre>                                                                            |
| <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>                  | <i>interface-name</i> —Name of the DFC interface.                                                                       |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 84</a></li></ul>          |

## interfaces (Video Monitoring)

```
Syntax interfaces {
 interface-name {
 family {
 inet {
 input-flows {
 input-flow-name {
 source-address [address];
 destination-address [address];
 source-port [port];
 destination-port [port];
 template template-name;
 }
 }
 }
 }
 }
 }
 }
 }
```

**Hierarchy Level** [edit services [video-monitoring](#)]

**Release Information** Statement introduced in Junos OS Release 14.1.

**Description** Define video monitoring for specified input or output flows on selected interfaces.

**Options** *interface-name*—Name of the interace to monitor.

*address*—Source or destination IPv4 address or prefix value.

*port*—Port number.

**Range:** 0 through 65,535

*template-name*—Name of the template used to monitor flows on an interface.

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 Inline Video Monitoring on page 311](#)

## inet6-options (Services)

---

|                                 |                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>inet6-options {<br/>    source-address <i>address</i>;<br/>}</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 14.1R4.                                                                                                                                                                                                                             |
| <b>Description</b>              | Specify the source IPv6 address used for probes. If the source IPv6 address is not one of the devices' assigned addresses, the packet will use the outgoing interface's address as its source.                                                                               |
| <b>Options</b>                  | <b>inet6-options</b> —Define the IPv6 protocol-related settings to be used for RPM probes<br><br><b>source-address <i>ipv6-address</i></b> —Specify the base IPv6 address to be used for sending the RPM probes from the client to the server (for example, ::ffff:a:b:c:d). |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 201</a></li></ul>                                                                                                                                                                         |

## ip-swap (RFC 2544 Benchmarking)

---

|                                 |                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ip-swap;</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 12.3X53 for ACX Series routers.<br>Statement introduced in Junos OS Release 14.2 for MX Series routers.                                                                                                                         |
| <b>Description</b>              | Swaps source and destination IPv4 addresses. This statement is applicable only for family <b>bridge</b> .                                                                                                                                                                |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li><li>• <a href="#">rfc2544-benchmarking on page 477</a></li></ul> |

## ipv4-flow-table-size

---

|                                 |                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ipv4-flow-table-size <i>units</i>;</code>                                                                                                       |
| <b>Hierarchy Level</b>          | <code>[edit chassis fpc <i>slot-number</i> inline-services flow-table-size]</code>                                                                    |
| <b>Description</b>              | Configure the size of the IPv4 flow table in units of 256K entries.                                                                                   |
| <b>Options</b>                  | <p><b><i>units</i></b>—Number of 256K flow entries available for the IPv4 flow table.</p> <p><b>Range:</b> 1 through 15</p> <p><b>Default:</b> 1K</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 Inline Active flow Monitoring on page 122</a></li> </ul>                             |

## ipv4-template

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ipv4-template;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <code>[edit <a href="#">services flow-monitoring version9 template <i>template-name</i></a>],</code><br><code>[edit <a href="#">services flow-monitoringversion-ipfix template <i>template-name</i></a>]</code>                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 8.3.</p> <p>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.</p> <p>Statement introduced in Junos OS Release 15.1F4 for PTX Series routers with third-generation FPCs installed. Supported at the <code>[edit <a href="#">services flow-monitoring version-ipfix template <i>template-name</i></a>]</code> hierarchy level.</p> |
| <b>Description</b>              | Specify that the flow aggregation version 9 or IPFIX template is used only for IPv4 records.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <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 Aggregation to Use Version 9 Flow Templates on page 137</a></li> <li>• <a href="#">Configuring Flow Aggregation to Use IPFIX Flow Templates on PTX Series Routers on page 152</a></li> </ul>                                                                                                                                                                                                                                 |


## ipv6-flow-table-size

---

|                                 |                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ipv6-flow-table-size <i>units</i>;</code>                                                                                         |
| <b>Hierarchy Level</b>          | [edit chassis fpc <i>slot-number</i> inline-services ipv6 flow-table-size]                                                              |
| <b>Description</b>              | Configure the size of the IPv6 flow table in units of 256K entries.                                                                     |
| <b>Options</b>                  | <b><i>units</i></b> —Number of 256K flow entries available for the IPv6 flow table.<br><b>Range:</b> 1 through 15<br><b>Default:</b> 1K |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Inline Active flow Monitoring on page 122</a></li></ul>                 |

## ipv6-extended-attrib

---

|                                 |                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ipv6-extended-attrib;</code>                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit chassis fpc <i>slot-number</i> inline-services ipv6 flow-table-size]                                                                                                                                                 |
| <b>Description</b>              | Enable the inclusion of element ID, 54, fragmentIdentification, and element ID, 64, ipv6ExtensionHeaders, in IPFIX flow templates that are exported to the flow collector                                                  |
|                                 | <div> <b>NOTE:</b> Collection of IPv4 fragmentation IDs occurs automatically without having to configure this setting explicitly.</div> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Inline Active flow Monitoring on page 122</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> ]                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.4.</p> <p>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.</p> <p>Statement introduced in Junos OS Release 15.1F4 for PTX Series routers with third-generation FPCs installed. Supported at the [edit <a href="#">services flow-monitoring version-ipfix template <i>template-name</i></a>] hierarchy level.</p> |
| <b>Description</b>              | Specify that the flow aggregation version 9 or IPFIX template is used only for IPv6 records.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Usage Guidelines</b>         | See “ <a href="#">Configuring Flow Aggregation to Use Version 9 Flow Templates</a> ” on page 137.                                                                                                                                                                                                                                                                                                                                                                        |
| <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 Aggregation to Use Version 9 Flow Templates on page 137</a></li> <li>• <a href="#">Configuring Flow Aggregation to Use IPFIX Flow Templates on PTX Series Routers on page 152</a></li> </ul>                                                                                                                                                                                                       |

## jflow-log (Interfaces)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>jflow-log {<br/>    message-rate-limit <i>messages-per-second</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <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 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Configure generation of log messages or template records in flow monitoring format for NAT error events. These records for NAT error events are generated when addresses for allocation from the NAT pool are not available, when ports for allocation to a subscriber are not available, or when the allocated quota is exceeded for NAT events (more than the configured number of ports is requested).                                                                                                                                |
| <b>Options</b>                  | The remaining statement is described separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li><li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li><li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li><li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</a></li></ul> |



## jflow-log (Services)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> jflow-log {     collector <i>collector-name</i> {         source-ip <i>address</i>;         destination-address <i>address</i>;         destination-port <i>port-number</i>;     }     collector-group <i>collector-group-name</i> {         [<i>collector-name1 collector-name2</i>];     }     template-profile <i>template-profile-name</i> {         collector <i>collector-name</i> ;         collector-group <i>collector-group-name</i> ;         template-type nat;         version (ipfix   v9);         refresh-rate <i>packets packets seconds seconds</i>;         message-rate-limit <i>messages-per-second</i>     } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit services]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | <p>Enable the mechanism to record logging messages in flow monitoring format for NAT events. For this transmission of flow monitoring logs to work properly, the services PIC interface must have an IP address and appropriate logging options configured.</p> <p>You can configure MX Series routers with MS-MPCs and MS-MICs to log network address translation (NAT) events using the Junos Traffic Vision (previously known as Jflow) version 9 or IPFIX (version 10) template format. This method of generating flow monitoring records for NAT events, such as NAT44 and NAT64 session creation and deletion, and NAT44 and NAT64 binding information base events, enables cohesive and streamlined analysis of NAT traffic and troubleshooting of NAT-related problems.</p> <p>Define the attributes for recording logging messages in flow template format for NAT events, such as a collector, template profile, and the properties for transmission of flow monitoring logs from an exporter to an external host or collector.</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="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li> <li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li> <li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li> <li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</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> ],<br>[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.<br>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 137</a></li></ul>                                                                           |

## license-server

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>license-server {   ip-address <i>address</i>;   log-interval <i>seconds</i>;   services (jflow   cgnat   firewall); }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1 for MX Series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | On MX Series routers with MS-MICs and MS-MPCs, configure the capability to transmit the throughput details per service for the Junos Address Aware, Junos Traffic Vision, and Junos Network Secure services in the last time interval to an external log collector.                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>ip-address <i>address</i></b>—Specify the IP address of the license log server.</p> <p><b>log-interval <i>seconds</i></b>—Specify the frequency at which throughput data must be sent from the router to the log collector.<br/> <b>Range:</b> 60–86400 seconds</p> <p><b>services</b>—Specify the services for which throughput data must be exported.</p> <ul style="list-style-type: none"> <li>• <b>jflow</b>—Inline flow monitoring service or Junos Traffic Vision.</li> <li>• <b>cgnat</b>—Carrier-grade NAT service or Junos Address Aware.</li> <li>• <b>firewall</b>—Stateful firewall or Junos Network Secure.</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="#">License Server Management for Throughput Data Export for NAT, Firewall, and Inline Flow Monitoring Services on page 223</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## local-dump

---

|                          |                                                                                                                                                                                                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | (local-dump   no-local-dump);                                                                                                                                                                                                                                                |
| Hierarchy Level          | [edit forwarding-options <b>sampling instance</b> <i>instance-name</i> <b>family</b> (inet   inet6   mpls) <b>output flow-server</b> <i>hostname</i> ],<br>[edit forwarding-options <b>sampling family</b> (inet   inet6   mpls) <b>output flow-server</b> <i>hostname</i> ] |
| Release Information      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                            |
| Description              | Enable collection of cflowd records in a log file.                                                                                                                                                                                                                           |
| Options                  | <b>no-local-dump</b> —Do not dump cflowd records to a log file before exporting.<br><br><b>local-dump</b> —Dump cflowd records to a log file before exporting.                                                                                                               |
| Required Privilege Level | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                      |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">Enabling Flow Aggregation on page 132</a></li></ul>                                                                                                                                                                      |

## logical-system

---

|                          |                                                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | logical-system <i>logical-system-name</i> {<br>[ <b>routing-instances</b> <i>instance-name</i> ];<br>}                       |
| Hierarchy Level          | [edit services rpm bgp]                                                                                                      |
| Release Information      | Statement introduced in Junos OS Release 7.6.                                                                                |
| Description              | Specify the logical system used by the probes.                                                                               |
| Options                  | <b>logical-system-name</b> —Logical system name.<br><br>The remaining statements are explained separately.                   |
| Required Privilege Level | interface—To view this statement in the configuration.<br>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 211</a></li></ul> |

## match

---

|                                 |                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>match <i>expression</i>;</code>                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">port-mirroring traceoptions file</a> ],<br>[edit forwarding-options <a href="#">sampling traceoptions file</a> ]                          |
| <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.<br>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 173</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 103</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.<br>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 210</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.<br><b>Range:</b> 1 through 64                                                                                                                                                                           |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 405</a></li><li>• <a href="#">Limiting the Number of Duplicates of a Packet on page 87</a></li></ul>                                                                                     |

## max-packets-per-second

|                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                  | <code>max-packets-per-second <i>number</i>;</code>                                                                                                             |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                         | [edit forwarding-options <a href="#">sampling input</a> ],<br>[edit forwarding-options <a href="#">sampling instance instance-name 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>  <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. </div> |                                                                                                                                                                |
| <b>Options</b>                                                                                                                                                                                                                                                                                                 | <i>number</i> —Maximum number of packets per second.<br><b>Range:</b> 0 through 65,535<br><b>Default:</b> 1000                                                 |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                | interface—To view this statement in the configuration.<br>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 103</a></li> </ul>                                                   |

## maximum-age

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>maximum-age <i>minutes</i>;</code>                                                                                |
| <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>                  | <i>minutes</i> —Transfer log file age.<br><b>Range:</b> 1 through 360                                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 38</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>         | Configure the maximum number of allowed connections between the server and all control client hosts. |




**NOTE:** The maximum number of connections between the server and all control client hosts must be greater than or equal to the number of connections between the server and a single controlled client host.

|                                 |                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b>                  | <code><i>count</i></code> —Maximum number of connections.<br><b>Range:</b> 1 through 1000<br><b>Default:</b> 64                                  |
| <b>Required Privilege Level</b> | <code>system</code> —To view this statement in the configuration.<br><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 TWAMP on page 210</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>                                                                                                                                                                                                                                                                                                      | Configure the maximum number of allowed connections between the server and a single control client host.             |
| <div>  <p><b>NOTE:</b> The maximum number of connections between the server and all control client hosts must be greater than or equal to the number of connections between the server and a single controlled client host.</p> </div> |                                                                                                                      |
| <b>Options</b>                                                                                                                                                                                                                                                                                                          | <i>count</i> —Maximum number of connections.<br><b>Range:</b> 1 through 500<br><b>Default:</b> 64                    |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                         | system—To view this statement in the configuration.<br>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 210</a></li> </ul>                    |

## maximum-packet-length

---

|                            |                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>maximum-packet-length bytes;</code>                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>     | [edit forwarding-options analyzer analyzer-name input],<br>[edit forwarding-options port-mirroring input],<br>[edit forwarding-options port-mirroring instance <i>instance-name</i> input],<br>[edit forwarding-options <a href="#">sampling input</a> ],<br>[edit forwarding-options <a href="#">sampling instance</a> <i>instance-name</i> <a href="#">input</a> ] |
| <b>Release Information</b> | Statement introduced in Junos OS Release 9.6.<br>Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.<br>The [edit forwarding-options analyzer analyzer-name input] hierarchy level for MX Series routers introduced in Junos OS Release 14.1.                                                                                  |
| <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 or PTX Series routers with third-generation FPCs installed.



**NOTE:** For MX Series routers 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.

Native analyzer sessions (that is, the [edit forwarding-options analyzer analyzer-name input] hierarchy level for MX Series routers) can be configured without specifying input parameters, which would mean that the instance uses default input values: `rate = 1` and `maximum-packet-length = 0`.

|                |                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b> | <i>bytes</i> —Maximum length (in bytes) of the mirrored packet or the sampled packet.<br><b>Range:</b> 0 through 9216<br><b>Default:</b> 0 |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|

For MX Series routers 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 `maximum-packet-length` value of zero represents that truncation is disabled, and the entire packet is mirrored or sampled.

**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](#)
- [Configuring Traffic Sampling on page 103](#)

## maximum-sessions

**Syntax** `maximum-sessions count;`

**Hierarchy Level** [edit services rpm twamp server]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Configure the maximum number of allowed test sessions the server can have running at one time.



**NOTE:** The maximum number of test sessions running on the server at one time must be greater than or equal to the maximum number of sessions the server can open on a single client connection.

**Options** *count*—Maximum number of sessions.  
**Range:** 1 through 2048  
**Default:** 64

**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 210](#)

## 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>         | Configure the maximum number of allowed sessions the server can open on a single client connection. |



**NOTE:** The maximum number of test sessions running on the server at one time must be greater than or equal to the maximum number of sessions the server can open on a single client connection.

---

|                                 |                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Options</b>                  | <code>count</code> —Maximum number of sessions.<br><b>Default:</b> 64                                                |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>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 210</a></li></ul>                      |

## media-loss-rate


|                                 |                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>media-loss-rate {   no-syslog-generation;   generate-snmp-traps;   storm-control {     count <i>number</i>;     interval <i>number</i>;   }   alarm-mode {     immediate;   } }</pre>                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit services]                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | <p>Configure the media loss rate. The media loss rate is the number of media packets lost over a configurable time interval (interval-duration) where the flow packets are packets carrying streaming application information. A single IP packet can contain zero or more streaming packets.</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="#">Inline Video Monitoring Overview on page 309</a></li> <li>• <a href="#">alarms on page 342</a></li> </ul>                                                                                                                                                                                              |

## media-rate-variation

---

|                                 |                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>media-rate-variation {<br/>    no-syslog-generation;<br/>    generate-snmp-traps;<br/>    storm-control {<br/>        count <i>number</i>;<br/>        interval <i>number</i>;<br/>    }<br/>    alarm-mode {<br/>        mdi-records-count <i>number</i>;<br/>        average;<br/>    }<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit services]                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                             |
| <b>Description</b>              | <p>Configure the media rate variation. The media rate variation is the difference between the expected packet rate and actual packet rate expressed as a percentage of the expected packet rate.</p> <p>The remaining statements are explained separately.</p>                                             |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Inline Video Monitoring Overview on page 309</a></li><li>• <a href="#">alarms on page 342</a></li></ul>                                                                                                                                                |

## message-rate-limit (Flow Monitoring Logs for NAT)

|                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                          | <code>message-rate-limit <i>messages-per-second</i></code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                 | [edit interfaces <i>interface-name</i> services-options jflow-log]                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>                                                                                                                                                                                                                                             | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>                                                                                                                                                                                                                                                     | Define the maximum number of logs or template records in flow monitoring format to be generated for NAT error events per second from the specified interface. These records for NAT error events are generated when addresses for allocation from the NAT pool are not available, when ports for allocation to a subscriber are not available, or when the allocated quota is exceeded for NAT events (more than the configured number of ports is requested).                                                                                |
| <div>  <b>NOTE:</b> The <code>message-rate-limit</code> option can be configured only for multiservices interfaces (<code>ms-x/x/x</code>) and not with other interface types. </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                                                                                                                                                                                                                                                         | <p><b><i>messages-per-second</i></b>—Maximum number of flow monitoring log messages per second for NAT error events that can be formatted and sent from the PIC to an external collector. The default rate is 10,000 for an external collector.</p> <p><b>Range:</b> 1 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="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li> <li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li> <li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li> <li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</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>value</b> —Minimum priority value; if not specified, defaults to 0.<br><b>Range:</b> 0 through 254                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 83</a></li></ul>                             |

## mode (RFC 2544 Benchmarking)

---

|                                 |                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>mode reflect;</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 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.<br>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 235</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">rfc2544-benchmarking on page 477</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 6](#)

## 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],<br>[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> test-name]<br>[edit services rpm twamp client control-connection control-client-name]                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.<br>Statement at the [edit <a href="#">services</a> rpm twamp client control-connection control-client-name] hierarchy level introduced in Junos OS Release 15.1 for MX Series 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.<br><b>Range:</b> 0 through 255                                                                                                                                                                                                                                                                                                            |
| <b>Usage Guidelines</b>         | See <i>Configuring RPM Probes</i> .                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 201</a></li></ul>                                                                                                                                                                                                                                                                                                   |

## mpls-ipv4-template

---

|                                 |                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>mpls-ipv4-template {<br/>    label-position [ <i>positions</i> ];<br/>}</code>                                                                 |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> <a href="#">flow-monitoring</a> <a href="#">version9</a> <a href="#">template</a> template-name]                      |
| <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.<br>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 137</a></li></ul>           |

## mpls-template

---

|                                 |                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>mpls-template {<br/>    label-position [ <i>positions</i> ];<br/>}</code>                                                              |
| <b>Hierarchy Level</b>          | [edit <a href="#">services flow-monitoring version9 template</a> <i>template-name</i> ]                                                      |
| <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.<br>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 137</a></li> </ul> |

## multiservice-options

---

|                                 |                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>multiservice-options {<br/>    (<a href="#">core-dump</a>   no-<a href="#">core-dump</a>);<br/>    (<a href="#">syslog</a>   no-<a href="#">syslog</a>);<br/>    flow-control-options {<br/>        down-on-flow-control;<br/>        dump-on-flow-control;<br/>        reset-on-flow-control;<br/>    }<br/>}</code> |
| <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.<br><br>The statements are explained separately.                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 6</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

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation** • [Configuring File Formats on page 37](#)

## next-hop (Forwarding Options)

**Syntax** next-hop *address*;

**Hierarchy Level** [edit forwarding-options **port-mirroring family** (inet | inet6) **output interface** *interface-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Specify the next-hop address for sending copies of packets to an analyzer.

**Options** *address*—IP address of the next-hop router.

**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 173](#)

## next-hop-group (Forwarding Options)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>next-hop-group <i>group-name</i> {<br/>    interface <i>interface-name</i> {<br/>        next-hop <i>address</i>;<br/>    }<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit forwarding-options]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | <p>Specify the next-hop address for sending copies of packets to an analyzer.</p> <p>It is implicitly assumed that a subgroup is up only if more than one interface in the subgroup is up.</p>                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b><i>address</i></b>—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.</p> <p><b><i>group-name</i></b>—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.</p> <p><b><i>interface-name</i></b>—Name of interface used to reach the next-hop destination.</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 173</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                               |

## 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],<br>[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>              | 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.<br><br>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. |
| <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.<br>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 178</a></li> </ul>                                                                                                                                                                                                                                                                                            |

## no-filter-check

---

|                                 |                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>no-filter-check;</code>                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">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>              | Disable filter checking on the port-mirroring interface.<br><br>This statement is required when you send port-mirrored traffic to a Tunnel PIC that has a filter applied to it. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 173</a></li> </ul>                                                                      |

## no-remote-trace (Trace Options)

---

|                                 |                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-remote-trace;                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">port-mirroring traceoptions</a> ],<br>[edit forwarding-options <a href="#">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.<br>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 110</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.<br>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 85</a></li></ul>                                 |



## no-syslog-generation

|                            |                                                |
|----------------------------|------------------------------------------------|
| <b>Syntax</b>              | no-syslog-generation;                          |
| <b>Hierarchy Level</b>     | [edit services]                                |
| <b>Release Information</b> | Statement introduced in Junos OS Release 15.1. |
| <b>Description</b>         | Disable system log generation.                 |



**NOTE:** If this statement is not configured, edit services generates a system log with respective severity level for values not within the configured range.

|                                 |                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Inline Video Monitoring Overview on page 309</a></li> <li>• <a href="#">alarms on page 342</a></li> </ul> |

## notification-targets

|                                 |                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | notification-targets <i>address port port-number</i> ;                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit services dynamic-flow-capture <i>capture-group client-name control-source 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>                  | <p><i>address</i>—Allowed destination IP address.</p> <p><i>port port-number</i>—Allowed destination UDP port number.</p>                                                           |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 83</a></li> </ul>                                                                       |

## 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 157</a></li><li>• <a href="#">Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 160</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

---

## one-way-hardware-timestamp

---

|                                 |                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | one-way-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 8.5.<br>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.<br>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 207</a></li><li>• <a href="#">destination-interface on page 369</a></li><li>• <a href="#">hardware-timestamp on page 407</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><br><code>[edit <a href="#">services flow-monitoring version9 template <i>template-name</i></a>]</code><br><code>[edit <a href="#">services flow-monitoring version-ipfix template <i>template-name</i></a>]</code>                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.3.<br>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.<br>Statement introduced in Junos OS Release 15.1F4 for PTX Series routers with third-generation FPCs installed. Supported at the <code>[edit <a href="#">services flow-monitoring version-ipfix template <i>template-name</i></a>]</code> hierarchy level. |
| <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.<br><b>Range:</b> 1 through 480,000<br><b>Default:</b> 4800<br><br><b><i>seconds</i></b> —Refresh rate, in number of seconds.<br><b>Range:</b> 10 through 600<br><b>Default:</b> 60                                                                                                                                                                                                                                       |
| <b>Usage Guidelines</b>         | See <a href="#">“Configuring Flow Aggregation to Use Version 9 Flow Templates”</a> on page 137.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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</a> on page 137</li></ul>                                                                                                                                                                                                                                                                                                                                          |

## options-template-id

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>options-template-id <i>id</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit <a href="#">services flow-monitoring version9 template <i>template-name</i></a> ],<br>[edit <a href="#">services flow-monitoringversion-ipfix template <i>template-name</i></a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <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.<br><b>Range:</b> 1024 through 65535                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 157</a></li> <li>• <a href="#">Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 160</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## 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**    interface—To view this statement in the configuration.  
**Level**    interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Discard Accounting on page 115](#)

## 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 6](#)

## output (Port Mirroring)

---

|                                 |                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>output {<br/>    interface <i>interface-name</i> {<br/>        next-hop <i>address</i>;<br/>    }<br/>    no-filter-check;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit forwarding-options <b>port-mirroring family</b> (inet   inet6)]                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                           |
| <b>Description</b>              | <p>Configure output interfaces and flow properties.</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 Port Mirroring on page 173</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 103](#)

---

## 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.

**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 6](#)

---

## passive-monitor-mode

---

**Syntax** `passive-monitor-mode;`

**Hierarchy Level** `[edit interfaces interface-name unit logical-unit-number]`

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** 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.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Enabling Passive Flow Monitoring on page 26](#)
- [multiservice-options on page 441](#)

## 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.<br>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 36</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.<br>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 38</a></li> </ul>                |

## peer-as-billing-template

---

|                                 |                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>peer-as-billing-template;</code>                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit <a href="#">services flow-monitoring version9 template</a> <i>template-name</i> ]                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4.                                                                                                                                                      |
| <b>Description</b>              | Enables the extraction of bandwidth usage information for billing purposes in PIC-based sampling configurations. This capability is supported on routers and applies only to IPv4 and IPv6 traffic. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 137</a></li></ul>                                                          |

## pic-memory-threshold

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>pic-memory-threshold percentage <i>percentage</i>;</code>                                                         |
| <b>Hierarchy Level</b>          | [edit <a href="#">services dynamic-flow-capture</a> <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.<br>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 86</a></li></ul>                     |

## pop-all-labels

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | pop-all-labels {<br>required-depth <i>number</i> ;<br>}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> atm-options mpls],<br>[edit interfaces <i>interface-name</i> fastether-options mpls],<br>[edit interfaces <i>interface-name</i> gigether-options mpls],<br>[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.<br>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 28</a></li> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                           |

## port (Flow Monitoring)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>port port-number;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">accounting name</a> <a href="#">output cflowd hostname</a> ],<br>[edit forwarding-options <a href="#">monitoring name family</a> inet <a href="#">output cflowd hostname</a> ],<br>[edit forwarding-options <a href="#">sampling instance instance-name family</a> (inet   inet6   mpls) <a href="#">output flow-server hostname</a> ],<br>[edit forwarding-options <a href="#">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>              | 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> | interface—To view this statement in the configuration.<br>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 132</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                      |

## port (RPM)

---

|                                 |                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>port number;</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.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>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.<br>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 206</a></li></ul>                                                                                                      |

## port (TWAMP)

---

|                                 |                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>port <i>number</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>              | TWAMP server listening port.                                                                                         |
| <b>Options</b>                  | <i>number</i> —Port number.<br><b>Range:</b> 1 through 65,535                                                        |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>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 210</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.

**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 173](#)

## post-cli-implicit-firewall

**Syntax** post-cli-implicit-firewall;

**Hierarchy Level** [edit services rpm twamp]

**Release Information** Statement introduced in Junos OS Release 15.1.

**Description** Ensure that the CLI configured (**explicit firewall**) takes precedence over the implicit firewall. The inline TWAMP client or server uses implicit firewall to achieve its functionality.



**NOTE:** Wrong configuration of CLI firewall can lead to improper functioning of inline TWAMP client or server. After you enable or disable this configuration statement, you must restart the router, or restart remote operation using the command `restart remote-operations`, for the operation to be effective.

On issuing the command `restart remote-operations` all TWAMP sessions (both client and server) are aborted. You must restart all the RPM sessions and all TWAMP sessions (both client and server).

**Default** The default for this configuration statement is in disabled status.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation** • [Two-Way Active Measurement Protocol Overview on page 201](#)

## pre-rewrite-tos

---

|                                 |                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | pre-rewrite-tos;                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">sampling</a> ]                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1.                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Preserve prenormalized type-of-service (ToS) value for egress sampled or mirrored packets. This configuration preserves the prerewrite ToS value for all forms of sampling, such as Routing Engine-based sampling, port mirroring, flow monitoring, and so on. This statement is effective for egress sampling only. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 103</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;
 inet6-options source-address ipv6-address;
 moving-average-size number;
 next-hop next-hop;
 one-way-hardware-timestamp;
 probe-count count;
 probe-interval seconds;
 probe-type type;
 routing-instance instance-name;
 source-address address;
 target (url url | address ipv4-address | inet6-url url | inet6-address ipv6-address);
 test-interval interval;
 thresholds
 {
 egress-time microseconds;
 ingress-time microseconds;
 jitter-egress microseconds;
 jitter-ingress microseconds;
 jitter-rtt microseconds;
 rtt microseconds;
 std-dev-egress microseconds;
 std-dev-ingress microseconds;
 std-dev-rtt microseconds;
 successive-loss count;
 total-loss count;
 }
 traps [trap-names];
 }
 }

```

**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.

|                           |                                                               |
|---------------------------|---------------------------------------------------------------|
| <b>Required Privilege</b> | system—To view this statement in the configuration.           |
| <b>Level</b>              | interface-control—To add this statement to the configuration. |

---

## probe-count

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>probe-count count;</code>                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit services rpm bgp],<br>[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> test-name],<br>[edit services rpm twamp client control-connection control-client-name test-session session-name]                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.<br>Support at the [edit services rpm twamp client control-connection control-client-name] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers. |
| <b>Description</b>              | Specify the number of probes within a test.                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <b>count</b> —1 through 15 for RPM, for TWAMP 1 through 4294967290.                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 211</a></li><li>• <a href="#">Configuring RPM Probes on page 201</a></li></ul>                                                                                                                                                                                                |

## probe-interval

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>probe-interval <i>interval</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm <a href="#">bgp</a> ],<br>[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> <i>test-name</i> ],<br>[edit <a href="#">services</a> rpm <a href="#">twamp</a> client control-connection <i>control-client-name</i> test-session <i>session-name</i> ]                                                                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.<br>Support at the [edit <a href="#">services</a> rpm <a href="#">twamp</a> client control-connection <i>control-client-name</i> ] hierarchy level introduced in Junos OS Release 15.1 for MX Series 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> | interface—To view this statement in the configuration.<br>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 211</a></li> <li>• <a href="#">Configuring RPM Probes on page 201</a></li> <li>• <a href="#">Two-Way Active Measurement Protocol Overview on page 201</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.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>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>                  | <i>limit</i> —Maximum number of concurrent probes allowed.<br><b>Range:</b> 1 through 500(PTX Series Packet Transport Routers only) 1 through 200<br><b>Default:</b> 100                                            |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 206</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 206](#)

## probe-type

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>probe-type type;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | <code>[edit services rpm bgp],</code><br><code>[edit <a href="#">services rpm probe owner test</a> test-name]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>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>                  | <p><b>type</b>—Specify one of the following probe type values:</p> <ul style="list-style-type: none"> <li>• <b>http-get</b>—(Not available at the <code>[edit services rpm bgp]</code> 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 <code>[edit services rpm bgp]</code> 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> | <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 BGP Neighbor Discovery Through RPM on page 211</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## rate (Forwarding Options)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>rate number;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit forwarding-options analyzer <i>analyzer-name</i> input],<br>[edit forwarding-options <a href="#">port-mirroring family</a> (inet   inet6) <a href="#">input</a> ],<br>[edit forwarding-options <a href="#">port-mirroring input</a> ],<br>[edit forwarding-options <a href="#">sampling input</a> ],<br>[edit forwarding-options <a href="#">sampling instance</a> <i>instance-name</i> <a href="#">input</a> ]                                                      |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.<br>Support at the [edit forwarding-options analyzer <i>analyzer-name</i> input] hierarchy level for MX Series routers introduced in Junos OS Release 14.1.                                                                                                                                                                  |
| <b>Description</b>              | <p>Set 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.</p> <p>Native analyzer sessions (that is, the [edit forwarding-options analyzer <i>analyzer-name</i> input] hierarchy level for MX Series routers) can be configured without specifying input parameters, which would mean that the instance uses default input values: rate = 1 and maximum-packet-length = 0.</p> |
| <b>Options</b>                  | <i>number</i> —Denominator of the ratio.<br><b>Range:</b> 1 through 65,535                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Usage Guidelines</b>         | See <a href="#">“Configuring Port Mirroring” on page 173</a> or <a href="#">“Configuring Traffic Sampling” on page 103</a> .                                                                                                                                                                                                                                                                                                                                               |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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>                   | receive-options-packets;                                                                                                |
| <b>Hierarchy Level</b>          | [edit <b>interfaces</b> <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> 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.<br>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 26</a></li> </ul>         |

## receive-ttl-exceeded

---


|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | receive-ttl-exceeded;                                                                                                   |
| <b>Hierarchy Level</b>          | [edit <b>interfaces</b> <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> 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.<br>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 26</a></li> </ul>         |

## refresh-rate (Flow Monitoring Logs for NAT)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | refresh-rate packets <i>packets</i> seconds <i>seconds</i> ;                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit services jflow-log template-profile <i>template-profile-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Specify the refresh rate for transmitting flow template records with version 9 and IPFIX templates for NAT events to the collector, in either packets or seconds.                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>packets</b>— Number of packets after which templates are sent to the collector.<br/><b>Range:</b> 1 through 480,000<br/><b>Default:</b> 4800</p> <p><b>seconds</b>—Number of seconds after which templates are sent to the collector<br/><b>Range:</b> 10 through 600<br/><b>Default:</b> 600</p>                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li><li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li><li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li><li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</a></li></ul> |

## reflect-mode (RFC2544 Benchmarking)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | reflect-mode (mac-rewrite   mac-swap   no-mac-swap );                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> test-name test-name]                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3X52 for ACX Series routers.<br>Statement introduced in Junos OS Release 14.2 for MX104 3D Universal Edge Routers.                                                                                                                                                                                                                              |
| <b>Description</b>              | Specify the reflection mode for the benchmarking test.                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <p><b>mac-rewrite</b>—(ACX Series routers only) Enable rewriting of the MAC address on the reflected frames. The MAC addresses specified in the source-mac-address and destination-mac-address options are used.</p> <p><b>mac-swap</b>—Swaps the source and destination MAC addresses in the test frame. This is the default behavior.</p>                                                 |
|                                 | <div>  <p><b>NOTE:</b> In bridge families, when the service type is ELAN, MAC addresses are swapped by default, on the reflected frames. And, when the service type is ELINE , MAC addresses are not swapped by default.</p> </div>                                                                        |
|                                 | <p><b>no-mac-swap</b>—Does not swap the source and destination MAC addresses in the test frame. The frame is returned to the originator without any modification to the MAC addresses.</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="#">RFC2544-Based Benchmarking Tests for E-LAN and E-Line Services Overview on page 231</a></li> <li>• <a href="#">rfc2544-benchmarking on page 477</a></li> <li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li> <li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li> </ul> |

## reflect-etype (RFC 2544 Benchmarking)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | reflect-etype <i>ethertype-value</i> ;                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarkingtests</a> test-name <i>test-name</i> ]                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3X53 for ACX Series routers.<br>Statement introduced in Junos OS Release 15.1 for MX104 3D Universal Edge routers.                                                                                                                                                                                            |
| <b>Description</b>              | Specify the EtherType to be used for reflection of the test frames. EtherType is a two-octet field in an Ethernet frame that defines the protocol in the frame payload. This statement is valid only if you configure the test mode to be a reflector. If you do not configure this statement, all EtherTypes are reflected.                              |
| <b>Options</b>                  | <b><i>ethertype-value</i></b> —Identifier for the EtherType. The EtherType value appears in the Ethernet type field of the packet. It specifies the protocol being transported in the Ethernet frame. For instance, the EtherType for IPv4 is 0x0800. So, if you specify the value as 2048, IPv4 packets are reflected.<br><b>Range:</b> 1 through 65,535 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">Supported RFC2544-Based Benchmarking Statements on MX104 Routers on page 234</a></li><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li></ul>                                      |

## required-depth

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>required-depth <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | <p>[edit interfaces <i>interface-name</i> atm-options mpls <a href="#">pop-all-labels</a>],</p> <p>[edit interfaces <i>interface-name</i> fastether-options mpls <a href="#">pop-all-labels</a>],</p> <p>[edit interfaces <i>interface-name</i> gigether-options mpls <a href="#">pop-all-labels</a>],</p> <p>[edit interfaces <i>interface-name</i> sonet-options mpls <a href="#">pop-all-labels</a>]</p>                                                                                                                            |
| <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> | <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="#">Passive Flow Monitoring for MPLS Encapsulated Packets on page 28</a></li> <li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></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.<br><b>Range:</b> 0 through 10                                  |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 39</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.<br><b>Range:</b> 0 through 60                           |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 39</a></li></ul>                 |

## rfc2544-benchmarking

```
Syntax rfc2544-benchmarking {
 tests{
 test-name test-name {
 test-interface interface-name;
 mode reflect;
 family (bridge| 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](#)]

**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 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.

Define the attributes for the RFC 2544-based benchmarking test to examine and analyze the performance characteristics of a network interconnecting device.

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 235](#)
- [RFC2544-Based Benchmarking Tests Overview on page 227](#)
- [show services rpm rfc2544-benchmarking on page 635](#)
- [show services rpm rfc2544-benchmarking test-id on page 640](#)

## 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><br><code>[edit services rpm twamp client control-connection <i>control-client-name</i>]</code>                                                                                                                                                                                            |
| <b>Release Information</b>                                                                                                                                                                                                                                                 | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.<br>Support at the <code>[edit services rpm twamp client control-connection <i>control-client-name</i>]</code> hierarchy level introduced in Junos OS Release 15.1 for MX Series routers. |
| <b>Description</b>                                                                                                                                                                                                                                                         | Specify the routing instance used by the probes. The routing instance is also applicable for control connection.                                                                                                                                                                                                                                                                                             |
| <div> <b>NOTE:</b> The media interface from where the TWAMP control and test or data packets arrive and exit the si- logical interface must be a part of the same routing instance.</div> |                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                                                                                                                                                                                                                                                             | <b><i>instance-name</i></b> —Routing instance configured at the <code>[edit routing-instance]</code> hierarchy level.<br><b>Default:</b> Internet (IPv4) routing table <code>inet.0</code> .                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                            | <code>interface</code> —To view this statement in the configuration.<br><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 201</a></li><li>• <a href="#">Two-Way Active Measurement Protocol Overview on page 201</a></li></ul>                                                                                                                                                                                                                      |



---

## routing-instance (cflowd)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>routing-instance <i>instance-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">sampling</a> family (inet   inet6   mpls) output flow-server <i>hostname</i> ]                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.3.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Configure a non-default VPN routing and forwarding (VRF) instance through which flow collectors can be reachable for inline flow monitoring. You cannot configure a flow collector to be reachable through non-default VRF instances for version 5 and version 8 flows. You must configure the routing instance to be a VRF instance by including the <code>instance-type vrf</code> statement at the [edit routing-instances <i>instance-name</i> ] hierarchy level. |
| <b>Options</b>                  | <i>instance-name</i> —Name of a routing instance that has been configured at the [edit routing-instance] hierarchy level.                                                                                                                                                                                                                                                                                                                                             |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Directing Traffic Sampling Output to a Server Running the cflowd Application</i></li></ul>                                                                                                                                                                                                                                                                                                                                 |

## routing-instance-list (TWAMP)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>routing-instance-list {<br/>    <i>instance-name</i> {<br/>        port <i>number</i>;<br/>    }<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit services rpm twamp server]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | Configure the Two-Way Active Measurement Protocol (TWAMP) servers on specific routing instances, instead of associating the TWAMP server at the system-level to apply to all routing instances configured on a router. The default routing instance is Internet routing table <b>inet.0</b> . If you do not specify a routing instance, the TWAMP probe applies to all routing instances. To apply the TWAMP probe to only the default routing instance, you must explicitly set the value of <i>instance-name</i> to default. If an interface is not part of any routing instance, the default port is used for TWAMP probes. You can configure up to 100 routing instances for a TWAMP server. |
| <b>Options</b>                  | <p><i>instance-name</i>—Name of the routing instance, a maximum of 31 characters.</p> <p><i>number</i>—Port number.</p> <p><b>Range:</b> 1 through 65,535</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | <p>system—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 TWAMP on page 210</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## routing-instances

---

|                                 |                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>routing-instances <i>instance-name</i>;</code>                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit services rpm bgp],<br>[edit services rpm bgp logical-system <i>logical-system-name</i> ]                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.6.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>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>                  | <i>instance-name</i> —A routing instance configured at the [edit routing-instances] hierarchy level.<br><b>Default:</b> Internet routing table <code>inet.0</code> .                                            |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 211</a></li> </ul>                                                                                  |

## rpm (Interfaces)

---

|                            |                                                                                                                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>rpm (client   server   twamp-client   twamp-server);</code>                                                                                                                             |
| <b>Hierarchy Level</b>     | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]                                                                                                                      |
| <b>Release Information</b> | Statement introduced in Junos OS Release 8.1.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 15.1 for MX Series routers. |
| <b>Description</b>         | Associate an RPM or TWAMP client (router or switch that originates RPM or TWAMP probes) or RPM or TWAMP server with a specified interface.                                                    |



**NOTE:** The TWAMP client is applicable only for si- interfaces.

---

|                                 |                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b>                  | <b><i>client</i></b> —Identifier for RPM client router or switch.<br><br><b><i>server</i></b> —Identifier for RPM server.<br><br><b><i>twamp-client</i></b> —Identifier for RPM TWAMP client router.<br><br><b><i>twamp-server</i></b> —Identifier for RPM TWAMP server. |
| <b>Required Privilege Level</b> | <b>interface</b> —To view this statement in the configuration.<br><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 Timestamping on page 207</a></li></ul>                                                                                                                                                               |

## rpm (Services)

```
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;
 }
 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);
 authentication-key-chain identifier {
 key-id identifier {
 secret password-string;
 }
 }
 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 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]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure BGP neighbor discovery through RPM.

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 BGP Neighbor Discovery Through RPM on page 211](#)

## run-length

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>run-length <i>number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">port-mirroring input</a> ],<br>[edit forwarding-options port-mirroring instance <i>port-mirroring-instance-name</i> input],<br>[edit forwarding-options port-mirroring family (inet inet6) <a href="#">input</a> ],<br>[edit forwarding-options <a href="#">sampling input</a> ],<br>[edit forwarding-options <a href="#">sampling instance instance-name input</a> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>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.<br><b>Range:</b> 0 through 20<br><b>Default:</b> 0                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Applying Forwarding Table Filters</a></li> <li>• <a href="#">Configuring Port Mirroring on page 173</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 103</a></li> </ul>                                                                                                                                                                |

## sample-once

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>sample-once;</code>                                                                                               |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">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.<br>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 103</a></li> </ul>            |

## 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-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.<br>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Configure traffic sampling.<br><br>The statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 103</a></li><li>• <a href="#">Applying Forwarding Table Filters</a></li><li>• <a href="#">Collecting Traffic Sampling Output in the Cisco Systems NetFlow Services Export Version 9 Format</a></li><li>• <a href="#">Directing Traffic Sampling Output to a Server Running the cflowd Application</a></li><li>• <a href="#">Configuring Port Mirroring</a></li><li>• <a href="#">Tracing Traffic-Sampling Operations</a></li></ul> |

---

## sampling (Interfaces)

---

|                                 |                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>sampling <i>direction</i>;</code>                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet],<br>[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.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Junos OS Services Interfaces Library for Routing Devices</a></li><li>• <a href="#">Configuring Flow Monitoring on page 6</a></li></ul>                                                                                                                              |

## 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.<br>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 210</a></li> </ul>                                                                                                                                                                                                                         |

## server-inactivity-timeout

|                                 |                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | server-inactivity-timeout <i>minutes</i> ;                                                                                                                                                 |
| <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 through 30 minutes</p> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 210</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.<br>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 83</a></li></ul>                             |

## service-type (RFC2544 Benchmarking)

---

|                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                    | <code>service-type (elan   eline) ;</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 12.3X53 for ACX Series routers.<br>Statement introduced in Junos OS Release 14.2 for MX104 3D Universal Edge Routers.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>                                                                                                                                                                                                                                                               | Mention the service under test. Possible values are <b>elan</b> and <b>eline</b> . This statement is applicable only for the bridge family or when the <b>mode</b> is configured as reflect. When the service type is <b>elan</b> , MAC addresses are swapped by default on the reflected frames. The <b>no-mac-swap</b> is not supported in this service type. When the service type is <b>eline</b> , MAC addresses are not swapped by default in the reflected frames. Use the <b>mac-swap</b> option to swap the addresses. |
| <div> <b>NOTE:</b> When you configure the Layer 2 reflection, you can specify the service type under test as ELINE if you want to simulate an ELINE service using bridge encapsulation.</div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                  | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"><li>• <a href="#">rfc2544-benchmarking on page 477</a></li><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li></ul>                                                                                                                                                                                                                                                        |

## services

---

|                                 |                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | services { ... }                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit]                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                            |
| <b>Description</b>              | Configure router services.<br><br>The underlying statements are explained separately.                                                        |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 137</a></li> </ul> |

## services

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | services rpm { ... }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>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>                  | rpm—Identifies the RPM set of rules statements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 211</a></li> <li>• <a href="#">Configuring RPM Probes on page 201</a></li> <li>• <a href="#">Configuring RPM Receiver Servers on page 206</a></li> <li>• <a href="#">Limiting the Number of Concurrent RPM Probes on page 206</a></li> <li>• <a href="#">Configuring RPM Timestamping on page 207</a></li> <li>• <a href="#">Configuring TWAMP on page 210</a></li> <li>• <a href="#">Enabling RPM for the Junos OS Extension-Provider Package on page 221</a></li> </ul> |

## services-options

**Syntax**

```

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;
 pba-interim-logging-interval seconds;
 reassembly-timeout
 session-limit {
 maximum number;
 rate new-sessions-per-second;
 cpu-load-threshold percentage;
 }
 session-timeout seconds;
 jflow-log {
 message-rate-limit messages-per-second;
 }
 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;
}

```

**Hierarchy Level** [edit interfaces *interface-name*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Define the service options to be applied on an interface.

**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**

- *Interface Properties*.

## 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.<br>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 83</a></li> </ul>                           |

## size

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>size bytes;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">port-mirroring</a> <a href="#">traceoptions</a> <i>file</i> ],<br>[edit forwarding-options <a href="#">sampling</a> <i>family</i> (inet   inet6   mpls) <a href="#">output</a> <i>file</i> ],<br>[edit forwarding-options <a href="#">sampling</a> <a href="#">traceoptions</a> <i>file</i> ]                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | <p>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.</p> <p>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.</p> |
| <b>Options</b>                  | <p><b>bytes</b>—Maximum size of each traffic sampling file or trace log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).</p> <p><b>Syntax:</b> <i>xk</i> to specify KB, <i>xm</i> to specify MB, or <i>xg</i> to specify GB</p> <p><b>Range:</b> 10 KB through the maximum file size supported on your router</p> <p><b>Default:</b> 1 MB for sampling data; 128 KB for log information</p>                                                                                                                                                                                                                                             |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 173</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 103</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.<br>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 82</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.<br>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 82</a></li><li>• <a href="#">soft-limit on page 494</a></li></ul> |



## source-address (Forwarding Options)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-address <i>address</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | <p>[edit forwarding-options <a href="#">accounting name</a> <a href="#">output interface interface-name</a>],</p> <p>[edit forwarding-options <a href="#">monitoring name family family</a> inet <a href="#">output interface interface-name</a>],</p> <p>[edit forwarding-options <a href="#">sampling instance instance-name family</a> (inet   inet6   mpls) <a href="#">output interface interface-name</a>],</p> <p>[edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) <a href="#">output interface interface-name</a>],</p> <p>[edit forwarding-options <a href="#">sampling instance instance-name family</a> inet <a href="#">output inline-jflow</a>]</p> |
| <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> | <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 115</a></li> <li>• <a href="#">Configuring Flow Monitoring on page 6</a></li> <li>• <a href="#">Configuring Traffic Sampling on page 103</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## source-address (Services)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-address <i>address</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm <a href="#">probe</a> <i>owner</i> <a href="#">test</a> <i>test-name</i> ]                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.                                                                                                                                                                                                                                                       |
| <b>Description</b>              | <p>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.</p> <p>The following addresses cannot be used for the source IP address used for probes:</p> <ul style="list-style-type: none"><li>• 0.0.0.0</li><li>• 127.0.0.0/8 (loopback)</li><li>• 224.0.0.0/4 (multicast)</li><li>• 255.255.255.255 (broadcast)</li></ul> |
| <b>Options</b>                  | <i>address</i> —Valid IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 201</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                      |

## source-addresses

---

|                                 |                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-addresses [ <i>addresses</i> ];</code>                                                                                                     |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> 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>                  | <i>address</i> —Allowed IP source address.                                                                                                              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 83</a></li></ul>                                             |

---

## source-id

---

|                                 |                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-id <i>source-id</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 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>                  | <b><i>source-id</i></b> —Specify a unique identifier for the source for version 9 flows.<br><b>Range:</b> 0 through 255                                                                                                                                                         |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 157</a></li><li>• <a href="#">Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 160</a></li></ul> |

## source-ip (Flow Monitoring Logs for NAT)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-ip address;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | <code>[edit services jflow-log collector <i>collector-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Specify the source IPv4 address of the services PIC interface to be used for generation of flow monitoring log messages in flow monitoring template format for NAT events.                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <b>address</b> —Valid IPv4 address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li><li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li><li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li><li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</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.<br>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.<br><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.<br><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 235</a></li> <li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li> <li>• <a href="#">rfc2544-benchmarking on page 477</a></li> </ul>                      |

## source-mac-address (RFC2544 Benchmarking)

|                                 |                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-mac-address <i>mac-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 12.3X53 for ACX Series routers.<br>Statement introduced in Junos OS Release 14.2 for MX104 3D Universal Edge Routers.                                                                                                               |
| <b>Description</b>              | Specify the source MAC address used in generated test frames. This parameter is applicable for a bridge family.                                                                                                                                                              |
| <b>Options</b>                  | <b><i>mac-address</i></b> —Source MAC address. Specify the MAC address as six hexadecimal bytes in one of the following formats: <i>nnnn.nnnn.nnnn</i> or <i>nn:nn:nn:nn:nn:nn</i> ; for example, 0011.2233.4455 or 00:11:22:33:44:55.                                       |
| <b>Required Privilege Level</b> | <b>interface</b> —To view this statement in the configuration.<br><b>interface-control</b> —To add this statement to the configuration.                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">rfc2544-benchmarking on page 477</a></li> <li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li> <li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</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.<br>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<br><b>Default:</b> 4041                                                                                                                                                                            |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 235</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">rfc2544-benchmarking on page 477</a></li></ul> |

## stamp

---

|                                 |                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>(stamp   no-stamp);</code>                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">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><i>no-stamp</i></b> —Do not include timestamps. This is the default.<br><b><i>stamp</i></b> —Include a timestamp with each line of packet sampling information.<br><b>Default:</b> No timestamp is included. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 103</a></li></ul>                                                                                                      |

## storm-control

---



|                                 |                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | storm-control {<br>count <i>number</i> ;<br>interval <i>number</i> ;<br>}                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit services]                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Configure the count and the interval to control the flooding of SNMP traps per flow.                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>count <i>number</i></b>—Use the specified maximum number of SNMP traps generated in the configured interval.</p> <p><b>interval <i>number</i></b>—Use the specified minimum time period, in seconds, between the generation of successive traps.</p> <p><b>Default:</b> The default count value is 1. The default interval is 1 second.</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="#">Inline Video Monitoring Overview on page 309</a></li> <li>• <a href="#">alarms on page 342</a></li> </ul>                                                                                                                                                                                    |

## syslog

---

|                                 |                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | (syslog   no-syslog);                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit <a href="#">interfaces</a> <i>mo-fpc/pic/port</i> <a href="#">multiservice-options</a> ]                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | <p>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.</p> <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> | <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 6</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 owner test <i>test-name</i>]</code><br><code>[edit services rpm twamp client control-connection <i>control-client-name</i> test-session <i>session-name</i>]</code>                                                                                                                                                                                                                       |
| <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 Packet Transport Routers.</p> <p>Support at the <code>[edit services rpm twamp client control-connection <i>control-client-name</i>]</code> hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.</p> |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                 | Specify the destination address or URL used for the probes.                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                     | <p><b>url <i>url</i></b>—For HTTP probe types, specify a fully formed URL that includes <b>http://</b> in the URL address. You can also specify an IPv6 address of a host in the URL to denote the destination or server to which the RPM probes must be sent.</p>                                                                                                                                                       |
| <p> <b>NOTE:</b> The <i>url</i> is for RPM only.</p>                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p><b>address <i>address</i></b>—For all probe types other than the HTTP probes, specify an IPv4 or an IPv6 address for the target host.</p>                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p> <b>NOTE:</b> Starting with Junos OS Release 14.2R2, the RPM client router (the router or switch that originates the RPM probes) can send probe packets to the RPM probe server (the device that receives the RPM probes) that contains an IPv6 address.</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 RPM Probes on page 201</a></li> <li>• <a href="#">Two-Way Active Measurement Protocol Overview on page 201</a></li> </ul>                                                                                                                                                                                                                               |



---

## tcp

---

|                                 |                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>tcp {<br/>    destination-interface <i>interface-name</i>;<br/>    port <i>port</i>;<br/>}</pre>                     |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm <a href="#">probe-server</a> ]                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches. |
| <b>Description</b>              | Specify the port information for the TCP server.<br><br>The remaining statements are explained separately.                |
| <b>Usage Guidelines</b>         | See <i>Configuring RPM Receiver Servers</i> .                                                                             |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |

## templates

```
Syntax templates {
 template-name {
 interval-duration interval-duration;
 inactive-timeout inactive-timeout;
 rate {
 (layer3 layer3-packets-per-second | media media-bits-per-second);
 }
 delay-factor {
 ;
 threshold {
 (info | warning | critical) delay-factor-threshold;
 }
 }
 media-loss-rate {
 disable;
 threshold {
 (info | warning | critical) percentage mlr-percentage | packet-count mlr-packet-count;
 }
 }
 media-rate-variation {
 disable;
 threshold {
 (info | warning | critical) mrp-variation;
 }
 }
 media-packets-count-in-layer3 media-packets-count-in-layer3;
 media-packet-size media-packet-size;
 }
 }
```

**Hierarchy Level** [edit services [video-monitoring](#)]

**Release Information** Statement introduced in Junos OS Release 14.1.

**Description** Configure the media delivery index template containing the measurement parameters for video monitoring.

**Options** **delay-factor**—Define delay factor syslog threshold levels.

***delay-factor-threshold***—Delay factor threshold in milliseconds. When the threshold is exceeded, a syslog message is generated.

**Default:** 0—Do not generate syslogs.

**Range:** 0 though 65535 milliseconds

**disable**—Disable logging for the threshold.

***inactive-timeout***—Number of seconds of flow inactivity after which time media delivery index statistics collection for a flow is terminated.

**Range:** 30 through 300 seconds

**info | warning | critical**—Level of syslog message generated when a threshold is exceeded.

**interval-duration**—Number of seconds after which time media delivery index flow monitoring statistics for the interval are reported.

**Range:** 1 through 50

**layer3-packets-per-second**—Layer 3 packet rate in IP packets per second.

**Range:** 0 through 4,294,967,295 pps

**media-bits-per-second**—Media bit rate for the stream in bits per second.

**media-loss-rate**—Define media loss rate syslog threshold levels.

**media-packets-count-in-layer-3**—Number of media packets in an IP packet.

**Range:** 1 through 32

**media-packet-size**—Size of media packet in bits.

**Default:** 188

**Range:** 1 through 2048

**media-rate-variation**—Define delay factor syslog threshold levels.

**mlr-packet-count**—Media loss rate threshold expressed as the number of packets dropped. When the threshold is exceeded, a syslog message is generated.

**mlr-percentage**—Media loss rate threshold expressed as the percentage of total packets dropped. When the threshold is exceeded, a syslog message is generated.

**Range:** 0 through 100

**mrv-variation**—Media rate variation threshold. The variation is the ratio of actual media rate to the configured media rate, expressed as a percentage.

**template-name**—Name of the template containing media delivery index measurement criteria. The template can be assigned to an 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 Inline Video Monitoring on page 311</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;  
              inet6-options;  
              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.  
[inet6-options](#) option added in Junos OS Release 14.1R4 for MX Series 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.

**Usage Guidelines**    See *Configuring RPM Probes*.

**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 201](#)

## 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.

**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 235](#)
- [RFC2544-Based Benchmarking Tests Overview on page 227](#)
- [rfc2544-benchmarking on page 477](#)

## 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> | interface—To view this statement in the configuration.<br>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 235</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">rfc2544-benchmarking on page 477</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## test-interval

|                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                          | <code>test-interval <i>frequency</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>                                                                                                                                                 | <code>[edit services rpm bgp],</code><br><code>[edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> <i>test-name</i>]</code><br><code>[edit services rpm twamp client control-connection <i>control-client-name</i>]</code>                                                                                                                                                                      |
| <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> <p>Support at the <code>[edit services rpm twamp client control-connection <i>control-client-name</i>]</code> hierarchy level introduced in Junos OS Release 15.1 for MX Series routers.</p> |
| <b>Description</b>                                                                                                                                                     | Specify the time to wait between tests, in seconds.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                                                                                                                                                         | <i>frequency</i> —Number of seconds, from 1 through 86,400.                                                                                                                                                                                                                                                                                                                                                                     |
| <div>  <b>NOTE:</b> For TWAMP, the number of seconds range from 1 through 255. </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 BGP Neighbor Discovery Through RPM on page 211</a></li> <li>• <a href="#">Configuring RPM Probes on page 201</a></li> </ul>                                                                                                                                                                                                                                    |

## test-name (RFC 2544 Benchmarking)

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | <pre>test-name <i>test-name</i> {<br/>    test-interface <i>interface-name</i>;<br/>    mode reflect;<br/>    family (inet   ccc);<br/>    destination-ipv4-address <i>address</i>;<br/>    destination-udp-port <i>port-number</i>;<br/>    source-ipv4-address <i>address</i>;<br/>    source-udp-port <i>port-number</i>;<br/>    direction (egress   ingress);<br/>}</pre> |
| Hierarchy Level          | [edit <a href="#">services</a> rpm <a href="#">rfc2544-benchmarking tests</a> ]                                                                                                                                                                                                                                                                                                |
| Release Information      | Statement introduced in Junos OS Release 13.3 for MX104 3D Universal Edge Routers.                                                                                                                                                                                                                                                                                             |
| Description              | 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.                                                      |
| Options                  | <b>test-name</b> —Specify a test name. The name can be up to 32 characters in length.<br><br>The remaining statements are explained separately.                                                                                                                                                                                                                                |
| Required Privilege Level | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                        |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">rfc2544-benchmarking on page 477</a></li></ul>                                                                                                       |



## test-session

---

|                                 |                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>test-session session-name {     data-fill-with zeros data;     data-size size;     dscp-code-point dscp-bits;     probe-count count;     probe-interval seconds;     target (url url   address address); }</pre> |
| <b>Hierarchy Level</b>          | [edit services rpm twamp client control connection <i>session-name</i> ]                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                        |
| <b>Description</b>              | Specify the test session details that includes the session name, the contents of the test packet, the data size, the probe details, and the target destination details.                                               |
| <b>Options</b>                  | <p><i>session-name</i>—Name of the session.</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="#">Two-Way Active Measurement Protocol Overview on page 201</a></li> </ul>                                                                                          |

## thresholds

|                            |                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>thresholds thresholds;</code>                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>     | [edit <code>services rpm probe owner test test-name</code> ],<br>[edit <code>services rpm twamp client control-connection control-client-name</code> ]                                                                                                                                                                                                                                                 |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for PTX Packet Series Transport Routers.<br>Support at the [edit <code>services rpm twamp client control-connection control-client-name</code> ] hierarchy level introduced in Junos OS Release 15.1 for MX Series routers. |
| <b>Description</b>         | 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.                                                                                                                                                                                                 |



**NOTE:** If you configure a value of zero using the *thresholds* option for a certain probe parameter, the generation of SNMP traps is disabled for the corresponding probe attribute. For example, if you specify the `set thresholds jitter-egress 0` statement, it denotes that traps are not triggered when the jitter in egress time threshold is met or exceeded.

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b> | <p><i>thresholds</i>—Specify one or more threshold measurements. The following options are supported:</p> <ul style="list-style-type: none"> <li>• <b>egress-time</b>—Measures maximum source-to-destination time per probe.</li> <li>• <b>ingress-time</b>—Measures maximum destination-to-source time per probe.</li> <li>• <b>jitter-egress</b>—Measures maximum source-to-destination jitter per test.</li> <li>• <b>jitter-ingress</b>—Measures maximum destination-to- source jitter per test.</li> <li>• <b>jitter-rtt</b>—Measures maximum jitter per test, from 0 through 60,000,000 microseconds.</li> <li>• <b>rtt</b>—Measures maximum round-trip time per probe, in microseconds.</li> <li>• <b>std-dev-egress</b>—Measures maximum source-to-destination standard deviation per test.</li> <li>• <b>std-dev-ingress</b>—Measures maximum destination-to-source standard deviation per test.</li> <li>• <b>std-dev-rtt</b>—Measures maximum standard deviation per test, in microseconds.</li> <li>• <b>successive-loss</b>—Measures successive probe loss count, indicating probe failure.</li> <li>• <b>total-loss</b>—Measures total probe loss count indicating test failure, from 0 through 15.</li> </ul> |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**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 201](#)
- [Two-Way Active Measurement Protocol Overview on page 201](#)

## traceoptions (Dynamic Flow Capture)

**Syntax** `traceoptions {  
     file filename <files number> <size size> <world-readable | non-world-readable>;  
 }`

**Hierarchy Level** [edit services dynamic-flow-capture]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Enable and define tracing options for dynamic flow capture events.

**Options** **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. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file.0*, then *trace-file.1*, 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 **size** option.

**Range:** 2 through 1000 files.

**Default:** 10 files.

**no-world-readable**—(Optional) Restrict access to the file.

**world-readable**—(Optional) Enable free access to the file.

**Required Privilege Level** interface—To view this statement in the configuration.  
 interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Junos Capture Vision on page 81](#)

## traceoptions (Forwarding Options)

---

|                                 |                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>traceoptions {<br/>    no-remote-trace;<br/>    file filename &lt;files number&gt; &lt;size bytes&gt; &lt;match expression&gt; &lt;world-readable  <br/>    no-world-readable&gt;;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">port-mirroring</a> ],<br>[edit forwarding-options <a href="#">sampling</a> ]                                                                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                   |
| <b>Description</b>              | Configure traffic sampling tracing operations.<br><br>The statements are explained separately.                                                                                                      |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 110</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 215](#)

---

## transfer

---

**Syntax** transfer {  
    record-level *number*;  
    timeout *seconds*;  
}

**Hierarchy Level** [edit services flow-collector file-specification variant *variant-number*]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Specify when to send the flow collection file. The file is sent when either of the two conditions is met.

**Options** record-level *number*—Number of flow collection files collected.  
  
timeout *seconds*—Timeout duration.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring File Formats on page 37](#)

---

## transfer-log-archive

---

|                                 |                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>transfer-log-archive {   archive-sites {     ftp:url {       password "password";       username username;     }   }   filename-prefix prefix;   maximum-age minutes; }</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.<br>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 38</a></li></ul>                                                                             |

## traps

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>traps traps;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>     | [edit <a href="#">services</a> rpm <a href="#">probe</a> owner <a href="#">test</a> test-name]<br>[edit services rpm twamp client control-connection control-client-name]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b> | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.<br>Support at the [edit <a href="#">services</a> rpm twamp client control-connection control-client-name] hierarchy level introduced in Junos OS Release 15.1 for MX Series 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>             | <b>traps</b> —Specify one or more traps. The following options are supported: <ul style="list-style-type: none"><li>• <b>control-connection-closed</b>—Generate traps when the control connection is closed.</li><li>• <b>egress-jitter-exceeded</b>—Generate traps when the jitter in egress time threshold is met or exceeded.</li><li>• <b>egress-std-dev-exceeded</b>—Generate traps when the egress time standard deviation threshold is met or exceeded.</li><li>• <b>egress-time-exceeded</b>—Generate traps when the maximum egress time threshold is met or exceeded.</li><li>• <b>ingress-jitter-exceeded</b>—Generate traps when the jitter in ingress time threshold is met or exceeded.</li><li>• <b>ingress-std-dev-exceeded</b>—Generate traps when the ingress time standard deviation threshold is met or exceeded.</li><li>• <b>ingress-time-exceeded</b>—Generate traps when the maximum ingress time threshold is met or exceeded.</li><li>• <b>jitter-exceeded</b>—Generate traps when the jitter in round-trip time threshold is met or exceeded.</li><li>• <b>probe-failure</b>—Generate traps when successive probe loss thresholds are crossed.</li><li>• <b>rtt-exceeded</b>—Generate traps when the maximum round-trip time threshold is met or exceeded.</li><li>• <b>std-dev-exceeded</b>—Generate traps when the round-trip time standard deviation threshold is met or exceeded.</li><li>• <b>test-completion</b>—Generate traps when a test is completed.</li><li>• <b>test-failure</b>—Generate traps when the total probe loss threshold is met or exceeded.</li><li>• <b>test-iteration-done</b>—Generate traps when all test sessions under control connections complete one test iteration.</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 201](#)
- [Two-Way Active Measurement Protocol Overview on page 201](#)

## tth

**Syntax** `tth hops;`

**Hierarchy Level** `[edit services dynamic-flow-capture capture-group client-name content-destination identifier]`

**Release Information** Statement introduced in Junos OS Release 7.4.

**Description** Time-to-live (TTL) value for the IP-IP header.

**Options** *hops*—TTL value.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring the Content Destination on page 82](#)

## twamp

```
Syntax twamp {
 server {
 authentication-mode mode;
 authentication-key-chain identifier {
 key-id identifier {
 secret password-string;
 }
 }
 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;
 routing-instance-list {
 instance-name {
 port number;
 }
 }
 server-inactivity-timeout minutes;
 }
}
```

**Hierarchy Level** [edit services rpm]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Configure the Two-Way Active Measurement Protocol (TWAMP) responder or sever settings 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.

TWAMP is an open protocol for measurement of two-way metrics. The host that initiates the TCP connection takes the roles of the control-client and (in the two-host implementation) the session-sender. Such a device is also called the TWAMP client. The host that acknowledges the TCP connection accepts the roles of a server and (in the two-host implementation) and the session-reflector. Such a device is also called the TWAMP server. The TWAMP-Test messages are exchanged between the session-sender and the session-reflector, and the TWAMP-Control messages are exchanged between the control-client and the server.

The following addresses cannot be used for the **client-list** source IP address used for probes:

- 0.0.0.0
- 127.0.0.0/8 (loopback)
- 224.0.0.0/4 (multicast)

- 255.255.255.255 (broadcast)

The remaining statements are described separately.

|                                 |                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>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 210</a></li> </ul>                    |

## 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.<br>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 210</a></li> </ul>                    |

## template (Forwarding Options)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | template <i>template-name</i> ;                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">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> ],<br>[edit forwarding-options <a href="#">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.<br>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 137</a></li> </ul>                                                                                                                                                                                                                                |

## template-id

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | template-id <i>id</i> ;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit <a href="#">services flow-monitoring version9 template <i>template-name</i></a> ],<br>[edit <a href="#">services flow-monitoringversion-ipfix template <i>template-name</i></a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <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.<br><b>Range:</b> 1024 through 65535                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 157</a></li><li>• <a href="#">Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows on page 160</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## template-profile (Flow Monitoring Logs for NAT)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | template-profile <i>template-profile-name</i> ;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit services jflow-log],<br>[edit services service-set <i>service-set-name</i> jflow-log]                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Specify the name of the flow template profile to be used for generating flow monitoring format messages for NAT events and for transmitting them to the collector. You can define a template profile for the Jflow service by using this statement at the <b>[edit services jflow-log]</b> hierarchy level, and associate the template profile with a service set by using this statement at the <b>[edit services service-set <i>service-set-name</i> jflow-log]</b> hierarchy level.                                                        |
| <b>Options</b>                  | <i>template-profile-name</i> —Name of the flow template profile for NAT events. The name can be up to 32 alphanumeric characters in length. Allowed characters are [a-zA-Z0-9_].                                                                                                                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li> <li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li> <li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li> <li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</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> ]<br>[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.<br>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.<br>Statement introduced in Junos OS Release 15.1F4 for PTX Series routers with third-generation FPCs installed. Supported at the [edit <a href="#">services flow-monitoring version-ipfix template <i>template-name</i></a> ] hierarchy level. |
| <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.<br><b>Range:</b> 1 through 480,000<br><b>Default:</b> 4800<br><br><b><i>seconds</i></b> —Refresh rate, in number of seconds.<br><b>Range:</b> 10 through 600<br><b>Default:</b> 600                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 137</a></li></ul>                                                                                                                                                                                                                                                                                                                  |

---


## template-type (Flow Monitoring Logs for NAT)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | template-type nat;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit services jflow-log template-profile <i>template-profile-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | Specify the type of service for which flow template profiles, in version or IPFIX format, must be used for generating flow monitoring format messages for NAT events and for transmitting them to the collector. Currently, you can configure only NAT events or services for generation of log messages in flow monitoring format.                                                                                                                                                                                                      |
| <b>Options</b>                  | <b>nat</b> —Specify that flow template profiles must be used for generation of flow monitoring logs for NAT events.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li><li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li><li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li><li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</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> <a href="#">services-options</a> ]                                                                                                                                                                                         |
| <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 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).                          |
| <hr/>                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                   |
| <div> <b>NOTE:</b> This feature is not supported for Broadband Edge subscribers (given that service PIC off load is not available with aggregate Ethernet (AE)).</div> <hr/> |                                                                                                                                                                                                                                                                   |
| <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.<br>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 23</a></li></ul>                                                                                                                                                                      |

## udp

---

|                                 |                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | udp {<br><a href="#">destination-interface</a> <i>interface-name</i> ;<br><a href="#">port</a> <i>port</i> ;<br>}         |
| <b>Hierarchy Level</b>          | [edit <a href="#">services</a> rpm <a href="#">probe-server</a> ]                                                         |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.3 for EX Series switches. |
| <b>Description</b>              | Specify the port information for the UDP server.<br><br>The remaining statements are explained separately.                |
| <b>Usage Guidelines</b>         | See <i>Configuring RPM Receiver Servers</i> .                                                                             |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |



---

## udp-tcp-port-swap (RFC 2544 Benchmarking)

---

|                                 |                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | udp-tcp-port-swap;                                                                                                                                                                                                                                                       |
| <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 12.3X53 for ACX Series routers.<br>Statement introduced in Junos OS Release 14.2 for MX104 3D Universal Edge routers.                                                                                                           |
| <b>Description</b>              | Swaps source and destination UDP ports in the test packets. Only UDP port swap and UDP over IPv4 traffic is supported.                                                                                                                                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">rfc2544-benchmarking on page 477</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li></ul> |

## unit

---

|                                 |                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>unit logical-unit-number {<br/>    family inet {<br/>        address address {<br/>            destination destination-address;<br/>        }<br/>        filter {<br/>            group filter-group-number;<br/>            input filter-name;<br/>            output filter-name;<br/>        }<br/>        sampling direction;<br/>    }<br/>}</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>• <i>Junos OS Network Interfaces Library for Routing Devices</i> for other statements that do not affect services interfaces.</li><li>• <i>Junos OS Network Interfaces Library for Routing Devices</i></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.<br>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 38</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.<br>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 37</a></li> </ul>                                                                             |

## version

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>version <i>format</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">accounting name</a> <a href="#">output flow-server hostname</a> ],<br>[edit forwarding-options <a href="#">sampling instance</a> <i>instance-name</i> <a href="#">family</a> (inet   inet6   mpls) <a href="#">output flow-server hostname</a> ],<br>[edit forwarding-options <a href="#">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>              | Specify the version format of the aggregated flows exported to a cflowd server.                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <i>format</i> —Format of the flows.<br><b>Values:</b> 5 or 8<br><b>Default:</b> 5                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 383</a></li><li>• <a href="#">Enabling Flow Aggregation on page 132</a></li></ul>                                                                                                                                                                                                                                                            |

## version (Flow Monitoring Logs for NAT)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>version (ipfix   v9);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | <code>[edit services jflow-log template-profile <i>template-profile-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Specify the flow template format, such as IPFIX or version 9, to be used for generating flow monitoring records for NAT events and for transmitting them to the collector.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b>ipfix</b>—Use the IPFIX flow template format for flow monitoring logs for NAT events.</p> <p><b>v9</b>—Use the version 9 flow template format for flow monitoring logs for NAT events.</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="#">Logging NAT Events in Flow Monitoring Format Overview on page 48</a></li> <li>• <a href="#">Guidelines for Configuring Log Generation of NAT Events in Flow Monitoring Record Format on page 57</a></li> <li>• <a href="#">Easy and Effective Monitoring of NAT Events by Logging NAT Operations in Flow Template Formats on page 68</a></li> <li>• <a href="#">Example: Configuring Logs in Flow Monitoring Format for NAT Events for Optimal Troubleshooting on page 69</a></li> </ul> |

## version9 (Forwarding Options)

|                                 |                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>version9 {   <b>template</b> <i>template-name</i>; }</pre>                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | <p><code>[edit forwarding-options <b>sampling instance</b> <i>instance-name</i> <b>family</b> (inet   inet6   mpls) <b>output flow-server</b> <i>hostname</i>],</code></p> <p><code>[edit forwarding-options <b>sampling family</b> (inet   inet6   mpls) <b>output flow-server</b> <i>hostname</i>]</code></p> |
| <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> | <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 Flow Aggregation to Use Version 9 Flow Templates on page 137</a></li> </ul>                                                                                                                                                                    |

## version-ipfix (Services)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>version-ipfix {<br/>    <b>template</b> <i>template-name</i> {<br/>        <b>flow-active-timeout</b> <i>seconds</i>;<br/>        <b>flow-inactive-timeout</b> <i>seconds</i>;<br/>        <b>ipv4-template</b>;<br/>        <b>ipv6-template</b>;<br/>        <b>option-refresh-rate</b> <i>packets packets seconds seconds</i>;<br/>        <b>template-refresh-rate</b> <i>packets packets seconds seconds</i>;<br/>    }<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit <a href="#">services flow-monitoring</a> ]                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.2.<br>Statement introduced in Junos OS Release 12.R3 for EX Series switches.<br>Statement introduced in Junos OS Release 15.1F4 for PTX Series routers with third-generation FPCs installed.                                                                                                                                                                                                      |
| <b>Description</b>              | Specify the output template properties to support inline flow monitoring. The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Inline Active flow Monitoring on page 122</a></li><li>• <a href="#">Configuring Inline Flow Monitoring on PTX Series Routers on page 127</a></li></ul>                                                                                                                                                                                                                        |

## video-monitoring

```
Syntax video-monitoring {
 templates {
 template-name {
 interval-duration interval-duration;
 inactive-timeout inactive-timeout;
 rate {
 (layer3 layer3-packets-per-second | media media-bits-per-second);
 }
 delay-factor {
 disable;
 threshold {
 (info | warning | critical) delay-factor-threshold;
 }
 }
 media-loss-rate {
 disable;
 threshold {
 (info | warning | critical) percentage mlr-percentage | packet-count
 mlr-packet-count;
 }
 }
 media-rate-variation {
 ;
 threshold {
 (info | warning | critical) mrw-variation;
 }
 }
 media-packets-count-in-layer3 media-packets-count-in-layer3;
 media-packet-size media-packet-size;
 }
 }
 interfaces {
 interface-name {
 family {
 inet {
 input-flows {
 input-flow-name {
 source-address [address];
 destination-address [address];
 source-port [port];
 destination-port [port];
 template template-name;
 }
 }
 output-flows {
 output-flow-name {
 source-address [address];
 destination-address [address];
 source-port [port];
 destination-port [port];
 template template-name;
 }
 }
 }
 }
 }
 }
}
```

```
 }
 }
}
```

|                                 |                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hierarchy Level</b>          | [edit services]                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1.                                                                                             |
| <b>Description</b>              | Define the options for video monitoring using media delivery index options for metrics. The remaining statements are explained separately. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Inline Video Monitoring on page 311</a></li></ul>                          |

---

## world-readable

---

|                                 |                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | (world-readable   no-world-readable);                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit forwarding-options <a href="#">port-mirroring traceoptions file</a> ],<br>[edit forwarding-options <a href="#">sampling family</a> (inet   inet6   mpls) <a href="#">output file</a> ],<br>[edit forwarding-options <a href="#">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.<br><br><b>world-readable</b> —Enable unrestricted file access.<br><br><b>Default:</b> no-world-readable                                                                                 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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 173</a></li><li>• <a href="#">Configuring Traffic Sampling on page 103</a></li></ul>                                                                                           |



## CHAPTER 16

# Operational Commands

- clear passive-monitoring statistics
- clear services accounting statistics inline-jflow
- clear services dynamic-flow-capture
- clear services flow-collector statistics
- clear services rpm twamp server connection
- clear services service-sets statistics jflow-log
- clear services video-monitoring mdi errors fpc-slot
- clear services video-monitoring mdi statistics fpc-slot
- request services flow-collector change-destination primary interface
- request services flow-collector change-destination secondary interface
- request services flow-collector test-file-transfer
- request services rpm twamp
- show forwarding-options next-hop-group
- show forwarding-options port-mirroring
- show interfaces (Dynamic Flow Capture)
- show interfaces (Flow Collector)
- show interfaces (Flow Monitoring)
- show passive-monitoring error
- show passive-monitoring flow
- show passive-monitoring memory
- show passive-monitoring status
- show passive-monitoring usage
- show services accounting aggregation
- show services accounting aggregation template
- show services accounting errors
- show services accounting flow
- show services accounting flow-detail
- show services accounting memory

- `show services accounting packet-size-distribution`
- `show services accounting status`
- `show services accounting usage`
- `show services dynamic-flow-capture content-destination`
- `show services dynamic-flow-capture control-source`
- `show services dynamic-flow-capture statistics`
- `show services flow-collector file interface`
- `show services flow-collector input interface`
- `show services flow-collector interface`
- `show services rpm active-servers`
- `show services rpm history-results`
- `show services rpm probe-results`
- `show services rpm rfc2544-benchmarking`
- `show services rpm rfc2544-benchmarking test-id`
- `show services rpm twamp client connection`
- `show services rpm twamp client history-results`
- `show services rpm twamp client probe-results`
- `show services rpm twamp client session`
- `show services rpm twamp server connection`
- `show services rpm twamp server session`
- `show services service-sets statistics jflow-log`
- `show services video-monitoring mdi errors fpc-slot`
- `show services video-monitoring mdi flows fpc-slot`
- `show services video-monitoring mdi stats fpc-slot`
- `test services rpm rfc2544-benchmarking test`

---

## clear passive-monitoring statistics

---

|                                 |                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear passive-monitoring statistics (all   interface <i>interface-name</i> )                                                                                                                                              |
| <b>Release Information</b>      | Command introduced in Junos OS Release 7.6.                                                                                                                                                                               |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Clear statistics for one passive monitoring interface or for all passive monitoring interfaces.                                                                  |
| <b>Options</b>                  | <b>all</b> —Clear statistics for all configured passive monitoring interfaces.<br><br><b>interface <i>interface-name</i></b> —Clear statistics for the specified passive monitoring interface ( <i>mo-fpc/pic/port</i> ). |
| <b>Required Privilege Level</b> | network                                                                                                                                                                                                                   |
| <b>List of Sample Output</b>    | <a href="#">clear passive-monitoring statistics on page 537</a>                                                                                                                                                           |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                     |

### Sample Output

#### clear passive-monitoring statistics

```
user@host> clear passive-monitoring statistics interface mo-5/0/0
```

## clear services accounting statistics inline-jflow

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear services accounting statistics inline-jflow<br><inline-jflow (fpc-slot <i>slot-number</i> )>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.2 for MX Series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | Clear inline flow statistics for a specified FPC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <b>fpc-slot <i>slot-number</i></b> —Clear inline flow statistics for the specified FPC. <ul style="list-style-type: none"><li>• MX80 routers only—Replace <i>slot-number</i> with a value from 0 through 1.</li><li>• MX104 routers only—Replace <i>slot-number</i> with a value from 0 through 2.</li><li>• MX240 routers only—Replace <i>slot-number</i> with a value from 0 through 2.</li><li>• MX480 routers only—Replace <i>slot-number</i> with a value from 0 through 5.</li><li>• MX960 routers only—Replace <i>slot-number</i> with a value from 0 through 11.</li><li>• MX2010 routers only—Replace <i>slot-number</i> with a value from 0 through 9.</li><li>• MX2020 routers only—Replace <i>slot-number</i> with a value from 0 through 19.</li></ul> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show services accounting flow on page 588</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

### Sample Output

#### clear services accounting statistics inline-jflow

```
user@host> user@host# run clear services accounting statistics inline-jflow fpc-slot 5
Statistics Cleared
```

## clear services dynamic-flow-capture

|                                 |                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear services dynamic-flow-capture capture-group <i>group-name</i><br><criteria-identifier <i>identifier</i> ><br><destination-identifier <i>identifier</i> ><br><force><br><static>                                                                                                                                                                                           |
| <b>Release Information</b>      | Command introduced in Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | (M320 routers and T Series routers only) Clear dynamic flow capture information for specified capture group.                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b>capture-group <i>group-name</i></b>—Capture-group identifier.</p> <p><b>criteria-identifier <i>identifier</i></b>—(Optional) Criteria identifier.</p> <p><b>destination-identifier <i>identifier</i></b>—(Optional) Content destination identifier.</p> <p><b>force</b>—(Optional) Force clearing of criteria.</p> <p><b>static</b>—(Optional) Clear static criteria.</p> |
| <b>Required Privilege Level</b> | network                                                                                                                                                                                                                                                                                                                                                                         |
| <b>List of Sample Output</b>    | <a href="#">clear services dynamic-flow-capture on page 539</a>                                                                                                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                           |

## Sample Output

### clear services dynamic-flow-capture

```
user@host> clear services dynamic-flow-capture capture-group flow-a
```

## clear services flow-collector statistics

---

|                                 |                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear services flow-collector statistics (all   interface <i>interface-name</i> )                                                                                                                                 |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                   |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Clear statistics for one flow collector interface or for all flow collector interfaces.                                                                  |
| <b>Options</b>                  | <b>all</b> —Clear statistics for all configured flow collector interfaces.<br><br><b>interface <i>interface-name</i></b> —Clear statistics for the specified flow collector interface ( <i>cp-fpc/pic/port</i> ). |
| <b>Required Privilege Level</b> | network                                                                                                                                                                                                           |
| <b>List of Sample Output</b>    | <a href="#">clear services flow-collector statistics on page 540</a>                                                                                                                                              |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                             |

### Sample Output

#### clear services flow-collector statistics

```
user@host> clear services flow-collector statistics interface cp-5/0/0
Flow collector interface: cp-5/0/0
Interface state: Collecting flows
Statistics cleared successfully
```

## clear services rpm twamp server connection

---

|                                 |                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>clear services rpm twamp server connection</b><br><i>&lt;connection-id&gt;</i>                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Clear connections established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control clients. By default all established connections are cleared (along with the sessions on those connections). To clear only a specific connection, specify the connection ID when you issue the command. |
| <b>Options</b>                  | <i>connection-id</i> —(Optional) Clear only the specified connection.                                                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                  |

## clear services service-sets statistics jflow-log

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear services service-sets statistics jflow-log<br><service-set <i>service-set-name</i> ><br><interface <i>interface-name</i> >                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Clear flow monitoring log statistics for the logs generated in IPFIX or version 9 format for one services interface or for all services interfaces, and for one named service set or all service sets on the interface or interfaces.                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <p><b>none</b>—Clear flow monitoring log for all configured services interfaces and their service sets.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Clear flow monitoring log statistics for the specified services interface. On M Series, MX Series, and T Series routers, the <i>interface-name</i> can be <b>ms-fpc/pic/port</b>. It is supported only on MS-MICs and MS-MPCS.</p> <p><b>service-set <i>service-set-name</i></b>—(Optional) Clear flow monitoring log statistics for the specified services interface.</p> |
| <b>Required Privilege Level</b> | network                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>show services service-sets statistics syslog</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">clear services service-sets statistics jflow-log on page 542</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Sample Output

### clear services service-sets statistics jflow-log

```
user@host> clear services service-sets statistics jflow-log interface ms-5/0/0
Interface: ms-5/0/0
```



## **clear services video-monitoring mdi errors fpc-slot**

---

|                                 |                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear services video-monitoring mdi errors fpc-slot <i>fpc-slot</i>                                                             |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1.                                                                                    |
| <b>Description</b>              | Clear all media delivery index error counters.                                                                                  |
| <b>Options</b>                  | <i>fpc-slot</i> —Number of the FPC slot.                                                                                        |
| <b>Required Privilege Level</b> | clear                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show services video-monitoring mdi stats fpc-slot on page 687</a></li></ul> |

## clear services video-monitoring mdi statistics fpc-slot

---

|                                 |                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear services video-monitoring mdi statistics fpc-slot <i>fpc-slot</i>                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1.                                                                                    |
| <b>Description</b>              | Clear all media delivery index statistics counters except for active flows.                                                     |
| <b>Options</b>                  | <i>fpc-slot</i> —Number of the FPC slot.                                                                                        |
| <b>Required Privilege Level</b> | clear                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show services video-monitoring mdi stats fpc-slot on page 687</a></li></ul> |

## request services flow-collector change-destination primary interface

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request services flow-collector change-destination primary interface <i>cp-fpc/pic/port</i><br><clear-files><br><clear-logs><br><immediately   gracefully>                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Switch to the primary File Transfer Protocol (FTP) server that is configured as a flow collector.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>none</b>—Switch to the primary FTP server.</p> <p><b>cp-fpc/pic/port</b>—Specify the flow collector interface name for the primary destination.</p> <p><b>clear-files</b>—(Optional) Request clearing of existing data files in the FTP wait queue when the switch takes place.</p> <p><b>clear-logs</b>—(Optional) Request clearing of existing logs when the switch takes place.</p> <p><b>immediately   gracefully</b>—(Optional) Specify whether you want the switch to take place immediately, or to affect only newly created files.</p> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">request services flow-collector change-destination primary interface on page 545</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

### Sample Output

#### request services flow-collector change-destination primary interface

```

user@host> request services flow-collector change-destination primary interface cp-6/0/0
Flow collector interface: cp-6/0/0
Interface state: Collecting flows
Destination change successful

```

## request services flow-collector change-destination secondary interface

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request services flow-collector change-destination secondary interface <i>cp-fpc/pic/port</i><br/>&lt;clear-files&gt;<br/>&lt;clear-logs&gt;<br/>&lt;immediately   gracefully&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Switch to the secondary File Transfer Protocol (FTP) server that is configured as a flow collector.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b>none</b>—Switch to the secondary FTP server.</p> <p><b><i>cp-fpc/pic/port</i></b>—Specify the flow collector interface name (<b><i>cp-fpc/pic/port</i></b>) for the secondary destination.</p> <p><b>clear-files</b>—(Optional) Request clearing of existing data files in the FTP wait queue when the switch takes place.</p> <p><b>clear-logs</b>—(Optional) Request clearing of existing logs when the switch takes place.</p> <p><b>immediately   gracefully</b>—(Optional) Specify whether you want the switch to take place immediately, or to affect only newly created files.</p> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>List of Sample Output</b>    | <a href="#">request services flow-collector change-destination secondary interface on page 546</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### Sample Output

#### request services flow-collector change-destination secondary interface

```
user@host> request services flow-collector change-destination secondary interface cp-6/0/0
Flow collector interface: cp-6/0/0
Interface state: Collecting flows
Destination change successful
```

## request services flow-collector test-file-transfer

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request services flow-collector test-file-transfer <i>filename</i> interface (all   <i>cp-fpc/pic/port</i>) (channel-zero   channel-one) (primary   secondary)</code>                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | (M40e, M160, and M320 routers, PTX Series, and T Series routers only) Transfer a test file to the primary or secondary File Transfer Protocol (FTP) server that is configured as a flow collector. This command verifies that the output side of the flow collector interface is operating properly.                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b><i>filename</i></b>—Name of the test file to transfer.</p> <p><b>interface all   <i>cp-fpc/pic/port</i></b>—Transfer a test file of flows from all configured flow collector interfaces or from only the specified interface.</p> <p><b>channel-zero   channel-one</b>—Transfer a file from export channel 0 (unit 0) or channel 1 (unit 1) of the PIC.</p> <p><b>primary   secondary</b>—Transfer a file to the primary or secondary server configured as a flow collector.</p> |
| <b>Required Privilege Level</b> | network                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>List of Sample Output</b>    | <a href="#">request services flow-collector test-file-transfer on page 547</a>                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                  |

## Sample Output

### request services flow-collector test-file-transfer

```
user@host> request services flow-collector test-file-transfer test_file interface cp-7/1/0
channel-one primary
```

```
Flow collector interface: cp-7/1/0
Interface state: Collecting flows
Response: Test file transfer successfully scheduled
```

## request services rpm twamp

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request services rpm twamp</code><br><code>&lt;start client <i>control-connection-name</i>&gt;</code><br><code>&lt;stop client <i>control-connection-name</i>&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 15.1 for MX Series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | <p>Start or stop a TWAMP session. You can start or stop all of the sessions for all of the TWAMP clients, or start or stop a session for a specific TWAMP client. When you start all the test session configured for a particular TWAMP client, the control-client initiates all requested testing with a Start-Sessions message, and the server sends an acknowledgment. If the control connection is not active between the server and the client, the control connection is also established and the test connections are started later. If the control-client name is not specified, all the configured test sessions are commenced.</p> <p>When you stop the test session, the control connection is closed only after the Stop-sessions message is sent from the TWAMP client to the TWAMP server. If the control-client name is not specified, all the configured test sessions are closed.</p> |
| <b>Options</b>                  | <p><b>start</b>—Start the TWAMP session between the TWAMP client and the TWAMP server.</p> <p><b>stop</b>—Terminate the TWAMP session between the TWAMP client and the TWAMP server.</p> <p><b><i>control-connection-name</i></b>—(Optional) Start or stop the TWAMP session with the server only for the specified control-connection or TWAMP control-client.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>List of Sample Output</b>    | <a href="#">request services rpm twamp start client control-connection-name on page 548</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### Sample Output

`request services rpm twamp start client control-connection-name`

```
user@host> request services rpm twamp start client c1
```

## show forwarding-options next-hop-group

|                                 |                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show forwarding-options next-hop-group</b><br><b>&lt;terse   brief   detail&gt;</b><br><b>&lt;group-name&gt;</b>                                                                                                               |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.6.<br>Command introduced in Junos OS Release 12.3R2 for EX Series switches.<br>Support for IPv6 introduced in Junos OS Release 14.2 for the MX Series routers.                           |
| <b>Description</b>              | Display current state of next-hop groups.                                                                                                                                                                                         |
| <b>Options</b>                  | <b>terse   brief   detail</b> —(Optional) Display the specified level of output.<br><br><b>group-name</b> —(Optional) Display a single next-hop group.                                                                            |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show forwarding-options port-mirroring on page 552</a></li> </ul>                                                                                                            |
| <b>List of Sample Output</b>    | <a href="#">show forwarding-options next-hop-group terse on page 550</a><br><a href="#">show forwarding-options next-hop-group brief on page 550</a><br><a href="#">show forwarding-options next-hop-group detail on page 550</a> |
| <b>Output Fields</b>            | <a href="#">Table 35 on page 549</a> lists the output fields for the <b>show forwarding-options next-hop-group</b> command. Output fields are listed in the approximate order in which they appear.                               |

**Table 35: show forwarding-options next-hop-group Output Fields**

| Field Name                           | Field Description                                                           | Level of Output     |
|--------------------------------------|-----------------------------------------------------------------------------|---------------------|
| <b>Next-hop-group</b>                | Name of next-hop group.                                                     | All levels          |
| <b>Type</b>                          | Next-hop group type, such as <b>inet</b> , <b>inet6</b> or <b>layer-2</b> . | All levels          |
| <b>State</b>                         | Next-hop group state, either <b>up</b> or <b>down</b> .                     | All levels          |
| <b>Members Interfaces</b>            | Names of interfaces to which next-hop group members belong.                 | <b>brief detail</b> |
| <b>Member Subgroup</b>               | Names of subgroups to which next-hop group members belong.                  | <b>brief detail</b> |
| <b>Number of members configured</b>  | Number of next-hop group members configured.                                | <b>detail</b>       |
| <b>Number of members that are up</b> | Number of next-hop group members that are up.                               | <b>detail</b>       |

Table 35: show forwarding-options next-hop-group Output Fields (*continued*)

| Field Name                      | Field Description                | Level of Output |
|---------------------------------|----------------------------------|-----------------|
| Number of subgroups configured  | Number of subgroups configured.  | detail          |
| Number of subgroups that are up | Number of subgroups that are up. | detail          |

## Sample Output

### show forwarding-options next-hop-group terse

```

user@host> show forwarding-options next-hop-group terse
Next-hop-group Type State
nhg inet up
nhg6 inet6 up
vpls_nhg_2 layer-2 down

```

### show forwarding-options next-hop-group brief

```

user@host> show forwarding-options next-hop-group brief

Next-hop-group: nhg
Type: inet
State: up
Members Interfaces:
 ge-0/2/8.0 next-hop 30.1.1.10
 ge-5/1/8.0 next-hop 10.1.1.10
 ge-5/1/9.0 next-hop 20.1.1.10

Next-hop-group: nhg6
Type: inet6
State: up
Members Interfaces:
 ge-5/1/5.0 next-hop 10::1:1:10
 ge-5/1/6.0 next-hop 20::1:1:10
Member Subgroup: nhsg6
Members Interfaces:
 ge-5/0/4.0 next-hop 3::1:1:1
 ge-5/1/4.0 next-hop 4::1:1:1

Next-hop-group: vpls_nhg_2
Type: layer-2 State: down

```

### show forwarding-options next-hop-group detail

```

user@host> show forwarding-options next-hop-group detail

Next-hop-group: nhg
Type: inet
State: up
Number of members configured : 3
Number of members that are up : 3
Number of subgroups configured : 0
Number of subgroups that are up : 0

```



```

Members Interfaces:
 ge-0/2/8.0 next-hop 30.1.1.10 up
 ge-5/1/8.0 next-hop 10.1.1.10 up
 ge-5/1/9.0 next-hop 20.1.1.10 up

Next-hop-group: nhg6
Type: inet6
State: up
Number of members configured : 2
Number of members that are up : 2
Number of subgroups configured : 1
Number of subgroups that are up : 1
Members Interfaces:
 ge-5/1/5.0 next-hop 10::1:1:10 up
 ge-5/1/6.0 next-hop 20::1:1:10 up
Member Subgroup: nhsg6
 Number of members configured : 2
 Number of members that are up : 2
 Members Interfaces:
 ge-5/0/4.0 next-hop 3::1:1:1 up
 ge-5/1/4.0 next-hop 4::1:1:1 up

Next-hop-group: vpls_nhg_2
Number of members configured : 2
Number of members that are up : 0
Number of subgroups configured : 0
Number of subgroups that are up : 0
Type: layer-2 State: down
Members Interfaces:
 ge-2/2/1.100 down
 ge-2/3/9.0 down

```

## show forwarding-options port-mirroring

|                                 |                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show forwarding-options port-mirroring</b><br><terse   detail><br><instance-name>                                                                                                                |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.6.<br>Command introduced in Junos OS Release 12.3R2 for EX Series switches.                                                                                |
| <b>Description</b>              | Display current state of port-mirroring instances.                                                                                                                                                  |
| <b>Options</b>                  | <b>terse   detail</b> —(Optional) Display the specified level of output.<br><br><b>instance-name</b> —(Optional) Display a single port-mirroring instance.                                          |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                |
| <b>Related Documentation</b>    |                                                                                                                                                                                                     |
| <b>List of Sample Output</b>    | <a href="#">show forwarding-options port-mirroring terse on page 553</a><br><a href="#">show forwarding-options port-mirroring detail on page 553</a>                                               |
| <b>Output Fields</b>            | <a href="#">Table 36 on page 552</a> lists the output fields for the <b>show forwarding-options port-mirroring</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 36: show forwarding-options port-mirroring Output Fields**

| Field Name               | Field Description                                   | Level of Output |
|--------------------------|-----------------------------------------------------|-----------------|
| Instance Name            | Name of port-mirroring instance.                    | All levels      |
| Instance Id              | Instance identification number.                     | All levels      |
| State                    | Instance state, either <b>up</b> or <b>down</b> .   | All levels      |
| <b>Input parameters</b>  |                                                     |                 |
| Rate                     | Rate (ratio of packets sampled).                    | <b>detail</b>   |
| Run-length               | Run length (number of consecutive packets sampled). | <b>detail</b>   |
| Maximum-packet-length    | Maximum packet length.                              | <b>detail</b>   |
| <b>Output parameters</b> |                                                     |                 |
| Family                   | Protocol family.                                    | <b>detail</b>   |
| State                    | Instance state, either <b>up</b> or <b>down</b> .   | <b>detail</b>   |
| Destination              | Destination (next-hop group name).                  | <b>detail</b>   |

## Sample Output

### show forwarding-options port-mirroring terse

```
user@host> show forwarding-options port-mirroring terse
Instance Name Instance Id State
&global_instance 1 up
inst1 2 up
```

### show forwarding-options port-mirroring detail

```
user@host> show forwarding-options port-mirroring detail
Instance Name: &global_instance
Instance Id: 1 State: up
 Input parameters:
 Rate: 10
 Run-length: 4
 Maximum-packet-length: 0
 Output parameters:
 Family: inet State: up Destination: inet_nhg
 Family: vpls/eth-switch State: up Destination: vpls_nhg

Instance Name: inst1
Instance Id: 2 State: up
 Input parameters:
 Rate: 1
 Run-length: 0
 Maximum-packet-length: 200
 Output parameters:
 Family: inet State: up Destination: inet_nhg
 Family: vpls/eth-switch State: down Destination: vpls_nhg_2
```

## show interfaces (Dynamic Flow Capture)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show interfaces dfc-fpc/pic/port:channel &lt;brief   detail   extensive   terse&gt; &lt;descriptions&gt; &lt;media&gt; &lt;snmp-index snmp-index&gt; &lt;statistics&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | (M320 and M120 routers and T Series routers only) Display status information about the specified dynamic flow capture interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <p><b>dfc-fpc/pic/port:channel</b>—Display standard status information about the specified dynamic flow capture interface.</p> <p><b>brief   detail   extensive   terse</b>—(Optional) Display the specified level of output.</p> <p><b>descriptions</b>—(Optional) Display interface description strings.</p> <p><b>media</b>—(Optional) Display media-specific information about network interfaces.</p> <p><b>snmp-index snmp-index</b>—(Optional) Display information for the specified SNMP index of the interface.</p> <p><b>statistics</b>—(Optional) Display static interface statistics.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>List of Sample Output</b>    | <a href="#">show interfaces (Dynamic Flow Capture) on page 557</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Output Fields</b>            | <a href="#">Table 37 on page 554</a> lists the output fields for the <b>show interfaces</b> (Dynamic Flow Capture) command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 37: Dynamic Flow Capture show interfaces Output Fields

| Field Name                | Field Description                                                                                                                    | Level of Output              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Physical Interface</b> |                                                                                                                                      |                              |
| <b>Physical interface</b> | Name of the physical interface.                                                                                                      | All levels                   |
| <b>Enabled</b>            | State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> . | All levels                   |
| <b>Interface index</b>    | Physical interface index number, which reflects its initialization sequence.                                                         | <b>detail extensive none</b> |
| <b>SNMP ifIndex</b>       | SNMP index number for the physical interface.                                                                                        | <b>detail extensive none</b> |
| <b>Type</b>               | Type of interface.                                                                                                                   | All levels                   |

Table 37: Dynamic Flow Capture show interfaces Output Fields (*continued*)

| Field Name                | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Level of Output         |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <b>Link-level type</b>    | Encapsulation type used on the physical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | All levels              |
| <b>MTU</b>                | Maximum Transmit Unit (MTU). Size of the largest packet to be transmitted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | All levels              |
| <b>Speed</b>              | Network speed on the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | All levels              |
| <b>Device flags</b>       | Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | All levels              |
| <b>Interface flags</b>    | Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | All levels              |
| <b>Link type</b>          | Data transmission type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | All levels              |
| <b>Link flags</b>         | Information about the link. Possible values are described in the “Link Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | All levels              |
| <b>Last flapped</b>       | Date, time, and how long ago the interface went from down to up. The format is <b>Last flapped: <i>year-month-day hour:minute:second timezone (hour:minute:second ago)</i></b> . For example, <b>Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail extensive</b> |
| <b>Input Rate</b>         | Input rate in bits per second (bps) and packets per second (pps).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | None specified          |
| <b>Output Rate</b>        | Output rate in bps and pps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | None specified          |
| <b>Traffic statistics</b> | <p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> <li>• <b>Input rate, Output rate</b>—Number of bits per second (packets per second) received and transmitted on the interface.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the interface.</li> </ul>                                                                                                                                                                                                                                                                                                                                                          | <b>detail extensive</b> |
| <b>Input errors</b>       | <ul style="list-style-type: none"> <li>• <b>Errors</b>—Input errors on the interface.</li> <li>• <b>Drops</b>—Number of packets dropped by the output queue of the I/O Manager ASIC.</li> <li>• <b>Framing errors</b>—Number of packets received with an invalid frame checksum (FCS).</li> <li>• <b>Runts</b>—Frames received smaller than the runt threshold.</li> <li>• <b>Giants</b>—Frames received larger than the giant threshold.</li> <li>• <b>Policed Discards</b>—Frames that the incoming packet match code discarded because the frames did not recognize them or were not of interest. Usually, this field reports protocols that the Junos OS does not support.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul> | <b>extensive</b>        |

Table 37: Dynamic Flow Capture show interfaces Output Fields (*continued*)

| Field Name                | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Level of Output              |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Output errors</b>      | <ul style="list-style-type: none"> <li>• <b>Carrier transitions</b>—Number of times the interface has gone from <b>down</b> to <b>up</b>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly, possibly once every 10 seconds, the cable, the remote system, or the interface is malfunctioning.</li> <li>• <b>Errors</b>—Sum of outgoing frame aborts and FCS errors.</li> <li>• <b>Drops</b>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet dropped by the ASIC RED mechanism.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul> | <b>extensive</b>             |
| <b>Logical Interface</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                              |
| <b>Logical interface</b>  | Name of the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | All levels                   |
| <b>Index</b>              | Logical interface index number, which reflects its initialization sequence.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>detail extensive none</b> |
| <b>SNMP ifIndex</b>       | Logical interface SNMP interface index number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail extensive none</b> |
| <b>Flags</b>              | Information about the logical interface; values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | All levels                   |
| <b>Encapsulation</b>      | Encapsulation on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | All levels                   |
| <b>Input packets</b>      | Number of packets received on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | None specified               |
| <b>Output packets</b>     | Number of packets transmitted on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | None specified               |
| <b>Traffic statistics</b> | <p>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the interface.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the interface.</li> </ul>                                                                                                                                                                                                     | <b>detail extensive</b>      |
| <b>Protocol</b>           | Protocol family configured on the logical interface (such as <b>iso</b> or <b>inet6</b> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>detail extensive none</b> |
| <b>MTU</b>                | MTU size on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>detail extensive none</b> |
| <b>Flags</b>              | Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>detail extensive none</b> |
| <b>Addresses, Flags</b>   | Addresses associated with the logical interface and information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>detail extensive none</b> |

Table 37: Dynamic Flow Capture show interfaces Output Fields (*continued*)

| Field Name         | Field Description                                | Level of Output              |
|--------------------|--------------------------------------------------|------------------------------|
| <b>Destination</b> | IP address of the remote side of the connection. | <b>detail extensive none</b> |
| <b>Local</b>       | IP address of the logical interface.             | <b>detail extensive none</b> |

## Sample Output

### show interfaces (Dynamic Flow Capture)

```

user@host> show interfaces dfc-0/0/0
Physical interface: dfc-0/0/0, Enabled, Physical link is Up
 Interface index: 146, SNMP ifIndex: 36
 Type: Adaptive-Services, Link-level type: Dynamic-Flow-Capture, MTU: 9192, Speed:
 2488320kbps
 Device flags : Present Running
 Interface flags: Point-To-Point SNMP-Traps 16384
 Link type : Full-Duplex
 Link flags : None
 Last flapped : 2005-08-26 15:08:36 PDT (01:18:42 ago)
 Input rate : 0 bps (0 pps)
 Output rate : 44800440 bps (100000 pps)

Logical interface dfc-0/0/0.0 (Index 67) (SNMP ifIndex 43)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Dynamic-Flow-Capture
 Input packets : 74
 Output packets: 132
 Protocol inet, MTU: 9192
 Flags: Receive-options, Receive-TTL-Exceeded
 Addresses, Flags: Is-Preferred Is-Primary
 Destination: 10.36.100.1, Local: 10.36.100.2

Logical interface dfc-0/0/0.1 (Index 68) (SNMP ifIndex 49)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Dynamic-Flow-Capture
 Input packets : 0
 Output packets: 402927263
 Protocol inet, MTU: 9192
 Flags: Receive-options, Receive-TTL-Exceeded

Logical interface dfc-0/0/0.2 (Index 69) (SNMP ifIndex 50)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Dynamic-Flow-Capture
 Input packets : 0
 Output packets: 0
 Protocol inet, MTU: 9192
 Flags: Receive-options, Receive-TTL-Exceeded

Logical interface dfc-0/0/0.16383 (Index 70) (SNMP ifIndex 44)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Dynamic-Flow-Capture
 Input packets : 1427
 Output packets: 98
 Protocol inet, MTU: 9192
 Flags: Receive-options, Receive-TTL-Exceeded
 Addresses, Flags: Is-Preferred Is-Primary
 Destination: 10.0.0.16, Local: 10.0.0.1

```

## show interfaces (Flow Collector)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show interfaces <i>cp-fpc/pic/port:channel</i> &lt;brief   detail   extensive   terse&gt; &lt;descriptions&gt; &lt;media&gt; &lt;snmp-index <i>snmp-index</i>&gt; &lt;statistics&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | (M Series and T Series routers only) Display status information about the specified flow collector interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b><i>cp-fpc/pic/port:channel</i></b>—Display standard status information about the specified flow collector interface.</p> <p><b>brief   detail   extensive   terse</b>—(Optional) Display the specified level of output.</p> <p><b>descriptions</b>—(Optional) Display interface description strings.</p> <p><b>media</b>—(Optional) Display media-specific information about network interfaces.</p> <p><b>snmp-index <i>snmp-index</i></b>—(Optional) Display information for the specified SNMP index of the interface.</p> <p><b>statistics</b>—(Optional) Display static interface statistics.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>List of Sample Output</b>    | <a href="#">show interfaces extensive (Flow Collector) on page 562</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | <a href="#">Table 38 on page 558</a> lists the output fields for the <b>show interfaces</b> (Flow Collector) command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                |

**Table 38: Flow Collector Show interfaces Output Fields**

| Field Name                | Field Description                                                                                                                           | Level of Output              |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Physical Interface</b> |                                                                                                                                             |                              |
| <b>Physical Interface</b> | Name of the physical interface type.                                                                                                        | All levels                   |
| <b>Link</b>               | Status of the link: <b>up</b> or <b>down</b> .                                                                                              | All levels                   |
| <b>Enabled</b>            | State of the interface type. Possible values are described in the “Enabled Devices” section under <i>Common Output Fields Description</i> . | All levels                   |
| <b>Interface index</b>    | Physical interface index number, which reflects its initialization sequence.                                                                | <b>detail extensive none</b> |
| <b>SNMP ifIndex</b>       | SNMP index number for the physical interface.                                                                                               | <b>detail extensive none</b> |



Table 38: Flow Collector Show interfaces Output Fields (*continued*)

| Field Name                     | Field Description                                                                                                                                                                                                                                                                                                                                     | Level of Output              |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Generation</b>              | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                                                                                     | <b>detail extensive</b>      |
| <b>Type</b>                    | Type of interface.                                                                                                                                                                                                                                                                                                                                    | All levels                   |
| <b>Link-level type</b>         | Encapsulation type used on the physical interface.                                                                                                                                                                                                                                                                                                    | All levels                   |
| <b>MTU</b>                     | Maximum Transmit Unit (MTU). Size of the largest packet to be transmitted.                                                                                                                                                                                                                                                                            | All levels                   |
| <b>Clocking</b>                | Reference clock source of the interface.                                                                                                                                                                                                                                                                                                              | All levels                   |
| <b>Speed</b>                   | Network speed on the interface.                                                                                                                                                                                                                                                                                                                       | All levels                   |
| <b>Device flags</b>            | Information about the physical device. Possible values are described in the "Device Flags" section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                    | All levels                   |
| <b>Interface flags</b>         | Information about the interface. Possible values are described in the "Interface Flags" section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                       | All levels                   |
| <b>Link type</b>               | Data transmission type.                                                                                                                                                                                                                                                                                                                               | All levels                   |
| <b>Link flags</b>              | Information about the link. Possible values are described in the "Link Flags" section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                 | All levels                   |
| <b>Physical info</b>           | Information about the physical interface.                                                                                                                                                                                                                                                                                                             | All levels                   |
| <b>Hold-times</b>              | Current interface hold-time up and hold-time down. Value is in milliseconds.                                                                                                                                                                                                                                                                          | <b>detail extensive none</b> |
| <b>Current address</b>         | Configured MAC address.                                                                                                                                                                                                                                                                                                                               | <b>detail extensive none</b> |
| <b>Hardware address</b>        | Media access control (MAC) address of the interface.                                                                                                                                                                                                                                                                                                  | <b>detail extensive none</b> |
| <b>Alternate link address</b>  | Backup link address.                                                                                                                                                                                                                                                                                                                                  | <b>detail extensive none</b> |
| <b>Last flapped</b>            | Date, time, and how long ago the interface went from down to up. The format is <b>Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago)</b> . For example, <b>Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)</b> .                                                                                                  | <b>detail extensive</b>      |
| <b>Statistics last cleared</b> | Time when the statistics for the interface were last set to zero.                                                                                                                                                                                                                                                                                     | <b>detail extensive</b>      |
| <b>Traffic statistics</b>      | Number and rate of bytes and packets received and transmitted on the physical interface. <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the interface.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the interface.</li> </ul> | <b>detail extensive</b>      |

Table 38: Flow Collector Show interfaces Output Fields (*continued*)

| Field Name                | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Level of Output              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Input errors</b>       | <ul style="list-style-type: none"> <li>• <b>Errors</b>—Input errors on the interface.</li> <li>• <b>Drops</b>—Number of packets dropped by the output queue of the I/O Manager ASIC.</li> <li>• <b>Framing errors</b>—Number of packets received with an invalid frame checksum (FCS).</li> <li>• <b>Runts</b>—Frames received smaller than the runt threshold.</li> <li>• <b>Giants</b>—Frames received larger than the giant threshold.</li> <li>• <b>Policed Discards</b>—Frames that the incoming packet match code discarded because the frames did not recognize them or were not of interest. Usually, this field reports protocols that Junos does not support.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul>                                                                                            | <b>extensive</b>             |
| <b>Output errors</b>      | <ul style="list-style-type: none"> <li>• <b>Carrier transitions</b> —Number of times the interface has gone from <b>down</b> to <b>up</b>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly, possibly once every 10 seconds, the cable, the remote system, or the interface is malfunctioning.</li> <li>• <b>Errors</b>—Sum of outgoing frame aborts and FCS errors.</li> <li>• <b>Drops</b>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet dropped by the ASIC RED mechanism.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul> | <b>extensive</b>             |
| <b>Logical Interface</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                              |
| <b>Logical interface</b>  | Name of the logical interface                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | All levels                   |
| <b>Index</b>              | Logical interface index number, which reflects its initialization sequence.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>detail extensive none</b> |
| <b>SNMP ifIndex</b>       | Logical interface SNMP interface index number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>detail extensive none</b> |
| <b>Generation</b>         | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>detail extensive</b>      |
| <b>Flags</b>              | Information about the logical interface; values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | All levels                   |
| <b>Encapsulation</b>      | Encapsulation on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | All levels                   |
| <b>Traffic statistics</b> | <p>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the interface.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the interface.</li> </ul>                                                                                                                                                                                                      | <b>detail extensive</b>      |

Table 38: Flow Collector Show interfaces Output Fields (*continued*)

| Field Name                | Field Description                                                                                                                                                                                                                                                                  | Level of Output              |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Local statistics</b>   | Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize. | <b>detail extensive</b>      |
| <b>Transit statistics</b> | Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.                               | <b>detail extensive</b>      |
| <b>Protocol</b>           | Protocol family configured on the logical interface (such as <b>iso</b> or <b>inet6</b> ).                                                                                                                                                                                         | <b>detail extensive none</b> |
| <b>MTU</b>                | MTU size on the logical interface.                                                                                                                                                                                                                                                 | <b>detail extensive none</b> |
| <b>Generation</b>         | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                  | <b>detail extensive</b>      |
| <b>Route table</b>        | Route table in which this address exists; for example, <b>Route table:0</b> refers to inet.0.                                                                                                                                                                                      | <b>detail extensive</b>      |
| <b>Flags</b>              | Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .                                                                                                                           | <b>detail extensive none</b> |
| <b>Addresses, Flags</b>   | Information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                | <b>detail extensive none</b> |
| <b>Destination</b>        | IP address of the remote side of the connection.                                                                                                                                                                                                                                   | <b>detail extensive none</b> |
| <b>Local</b>              | IP address of the logical interface.                                                                                                                                                                                                                                               | <b>detail extensive none</b> |
| <b>Broadcast</b>          | Broadcast address.                                                                                                                                                                                                                                                                 | <b>detail extensive none</b> |
| <b>Generation</b>         | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                  | <b>detail extensive</b>      |

## Sample Output

### show interfaces extensive (Flow Collector)

```

user@host> show interfaces extensive cp-5/0/0
Physical interface: cp-5/0/0, Enabled, Physical link is Up
 Interface index: 145, SNMP ifIndex: 52, Generation: 29
 Type: Flow-collector, Link-level type: Flow-collection, MTU: 9192,
 Clocking: Unspecified, Speed: 800mbps
 Device flags : Present Running
 Interface flags: Point-To-Point SNMP-Traps 16384
 Link type : Full-Duplex
 Link flags : None
 Physical info : Unspecified
 Hold-times : Up 0 ms, Down 0 ms
 Current address: Unspecified, Hardware address: Unspecified
 Alternate link address: Unspecified
 Last flapped : 2005-05-24 16:48:11 PDT (00:12:04 ago)
 Statistics last cleared: Never
 Traffic statistics:
 Input bytes : 2041661287 0 bps
 Output bytes : 3795049544 43816664 bps
 Input packets : 1365534 0 pps
 Output packets: 3865644 3670 pps
 Input errors:
 Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
 Policed discards: 0, Resource errors: 0
 Output errors:
 Carrier transitions: 2, Errors: 0, Drops: 0, MTU errors: 0,
 Resource errors: 0

Logical interface cp-5/0/0.0 (Index 74) (SNMP ifIndex 53) (Generation 28)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Flow-collection
 Traffic statistics:
 Input bytes : 1064651568
 Output bytes : 37144290
 Input packets : 711324
 Output packets: 713672
 Local statistics:
 Input bytes : 0
 Output bytes : 0
 Input packets : 0
 Output packets: 0
 Transit statistics:
 Input bytes : 1064651568 0 bps
 Output bytes : 37144290 0 bps
 Input packets : 711324 0 pps
 Output packets: 713672 0 pps
 Protocol inet, MTU: 9192, Generation: 39, Route table: 0
 Flags: Receive-options, Receive-TTL-Exceeded
 Addresses, Flags: Is-Preferred Is-Primary
 Destination: 4.0.0.2, Local: 4.0.0.1, Broadcast: Unspecified,
 Generation: 40

Logical interface cp-5/0/0.1 (Index 75) (SNMP ifIndex 54) (Generation 29)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Flow-collection
 Traffic statistics:
 Input bytes : 976793823
 Output bytes : 34099481
 Input packets : 652729
 Output packets: 655127

```

```

Local statistics:
 Input bytes : 0
 Output bytes : 0
 Input packets: 0
 Output packets: 0
Transit statistics:
 Input bytes : 976793823 0 bps
 Output bytes : 34099481 0 bps
 Input packets: 652729 0 pps
 Output packets: 655127 0 pps
Protocol inet, MTU: 9192, Generation: 40, Route table: 0
 Flags: Receive-options, Receive-TTL-Exceeded
 Addresses, Flags: Is-Preferred Is-Primary
 Destination: 4.1.1.2, Local: 4.1.1.1, Broadcast: Unspecified,
 Generation: 42

Logical interface cp-5/0/0.2 (Index 80) (SNMP ifIndex 55) (Generation 30)
 Flags: Point-To-Point SNMP-Traps Encapsulation: Flow-collection
 Traffic statistics:
 Input bytes : 0
 Output bytes : 3723079376
 Input packets: 0
 Output packets: 2495372
 Local statistics:
 Input bytes : 0
 Output bytes : 0
 Input packets: 0
 Output packets: 0
 Transit statistics:
 Input bytes : 0 0 bps
 Output bytes : 3723079376 43816664 bps
 Input packets: 0 0 pps
 Output packets: 2495372 3670 pps
 Protocol inet, MTU: 9192, Generation: 41, Route table: 0
 Flags: Receive-options, Receive-TTL-Exceeded
 Addresses, Flags: Is-Preferred Is-Primary
 Destination: 4.2.2.2, Local: 4.2.2.1, Broadcast: Unspecified,
 Generation: 44

Logical interface cp-5/0/0.16383 (Index 81) (SNMP ifIndex 56) (Generation 31)
...

```

## show interfaces (Flow Monitoring)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show interfaces mo-fpc/pic/port:channel &lt;brief   detail   extensive   terse&gt; &lt;descriptions&gt; &lt;media&gt; &lt;snmp-index snmp-index&gt; &lt;statistics&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | (M Series and T Series routers only) Display status information about the specified flow monitoring interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>                  | <p><b>mo-fpc/pic/port:channel</b>—Display standard status information about the specified flow monitoring interface.</p> <p><b>brief   detail   extensive   terse</b>—(Optional) Display the specified level of output.</p> <p><b>descriptions</b>—(Optional) Display interface description strings.</p> <p><b>media</b>—(Optional) Display media-specific information about network interfaces.</p> <p><b>snmp-index snmp-index</b>—(Optional) Display information for the specified SNMP index of the interface.</p> <p><b>statistics</b>—(Optional) Display static interface statistics.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>List of Sample Output</b>    | <a href="#">show interfaces extensive (Flow Monitoring) on page 567</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Output Fields</b>            | <a href="#">Table 39 on page 564</a> lists the output fields for the <b>show interfaces</b> (Flow Monitoring) command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table 39: show interfaces Output Fields (Flow Monitoring)**

| Field Name                | Field Description                                                                                                                    | Level of Output              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Physical Interface</b> |                                                                                                                                      |                              |
| <b>Physical interface</b> | Name of the physical interface.                                                                                                      | All levels                   |
| <b>Link</b>               | Status of the link: <b>up</b> or <b>down</b> .                                                                                       | All levels                   |
| <b>Enabled</b>            | State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> . | All levels                   |
| <b>Interface index</b>    | Physical interface index number, which reflects its initialization sequence.                                                         | <b>detail extensive none</b> |
| <b>SNMP ifIndex</b>       | SNMP index number for the physical interface.                                                                                        | <b>detail extensive none</b> |

Table 39: show interfaces Output Fields (Flow Monitoring) (*continued*)

| Field Name                     | Field Description                                                                                                                                                                                                                                  | Level of Output              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Generation</b>              | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                  | <b>detail extensive</b>      |
| <b>Description</b>             | Description and name of the interface.                                                                                                                                                                                                             | All levels                   |
| <b>Type</b>                    | Type of interface.                                                                                                                                                                                                                                 | All levels                   |
| <b>Link-level type</b>         | Encapsulation type used on the physical interface.                                                                                                                                                                                                 | All levels                   |
| <b>MTU</b>                     | Maximum Transmit Unit (MTU). Size of the largest packet to be transmitted.                                                                                                                                                                         | All levels                   |
| <b>Clocking</b>                | Reference clock source of the interface.                                                                                                                                                                                                           | All levels                   |
| <b>Speed</b>                   | Network speed on the interface.                                                                                                                                                                                                                    | All levels                   |
| <b>Device flags</b>            | Information about the physical device. Possible values are described in the "Device Flags" section under <i>Common Output Fields Description</i> .                                                                                                 | All levels                   |
| <b>Interface flags</b>         | Information about the interface. Possible values are described in the "Interface Flags" section under <i>Common Output Fields Description</i> .                                                                                                    | All levels                   |
| <b>Link type</b>               | Data transmission type.                                                                                                                                                                                                                            | All levels                   |
| <b>Link flags</b>              | Information about the link. Possible values are described in the "Link Flags" section under <i>Common Output Fields Description</i> .                                                                                                              | All levels                   |
| <b>Physical info</b>           | Information about the physical interface.                                                                                                                                                                                                          | All levels                   |
| <b>Hold-times</b>              | Current interface hold-time up and hold-time down. Value is in milliseconds.                                                                                                                                                                       | <b>detail extensive</b>      |
| <b>Current address</b>         | Configured MAC address.                                                                                                                                                                                                                            | <b>detail extensive none</b> |
| <b>Hardware address</b>        | Media access control (MAC) address of the interface.                                                                                                                                                                                               | <b>detail extensive none</b> |
| <b>Alternate link address</b>  | Backup link address.                                                                                                                                                                                                                               | <b>detail extensive none</b> |
| <b>Last flapped</b>            | Date, time, and how long ago the interface went from down to up. The format is <b>Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago)</b> . For example, <b>Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)</b> | <b>detail extensive</b>      |
| <b>Statistics last cleared</b> | Time when the statistics for the interface were last set to zero.                                                                                                                                                                                  | <b>detail extensive</b>      |

Table 39: show interfaces Output Fields (Flow Monitoring) (*continued*)

| Field Name                | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Level of Output              |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Traffic statistics</b> | <p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the interface.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the interface.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>detail extensive</b>      |
| <b>Input errors</b>       | <ul style="list-style-type: none"> <li>• <b>Errors</b>—Input errors on the interface.</li> <li>• <b>Drops</b>—Number of packets dropped by the output queue of the I/O Manager ASIC.</li> <li>• <b>Framing errors</b>—Number of packets received with an invalid frame checksum (FCS).</li> <li>• <b>Runts</b>—Frames received smaller than the runt threshold.</li> <li>• <b>Giants</b>—Frames received larger than the giant threshold.</li> <li>• <b>Policed Discards</b>—Frames that the incoming packet match code discarded because the frames did not recognize them or were not of interest. Usually, this field reports protocols that Junos does not support.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul>                                                                                           | <b>extensive</b>             |
| <b>Output errors</b>      | <ul style="list-style-type: none"> <li>• <b>Carrier transitions</b>—Number of times the interface has gone from <b>down</b> to <b>up</b>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly, possibly once every 10 seconds, the cable, the remote system, or the interface is malfunctioning.</li> <li>• <b>Errors</b>—Sum of outgoing frame aborts and FCS errors.</li> <li>• <b>Drops</b>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet dropped by the ASIC Red mechanism.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul> | <b>extensive</b>             |
| <b>Logical Interface</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                              |
| <b>Logical interface</b>  | Name of the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | All levels                   |
| <b>Index</b>              | Logical interface index number, which reflects its initialization sequence.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>detail extensive none</b> |
| <b>SNMP ifIndex</b>       | Logical interface SNMP interface index number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail extensive none</b> |
| <b>Generation</b>         | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <b>detail extensive</b>      |
| <b>Flags</b>              | Information about the logical interface; values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | All levels                   |
| <b>Encapsulation</b>      | Encapsulation on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | All levels                   |



Table 39: show interfaces Output Fields (Flow Monitoring) (*continued*)

| Field Name                | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Level of Output              |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Traffic statistics</b> | <p>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the interface.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the interface.</li> </ul> | <b>detail extensive</b>      |
| <b>Local statistics</b>   | Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.                                                                                                                                                                                                                                                                                                                                                | <b>detail extensive</b>      |
| <b>Transit statistics</b> | Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.                                                                                                                                                                                                                                                                                                                                                                              | <b>detail extensive</b>      |
| <b>Protocol</b>           | Protocol family configured on the logical interface (such as <b>iso</b> or <b>inet6</b> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail extensive none</b> |
| <b>MTU</b>                | MTU size on the logical interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>detail extensive none</b> |
| <b>Generation</b>         | Unique number for use by Juniper Networks technical support only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>detail extensive</b>      |
| <b>Route table</b>        | Route table in which this address exists; for example, <b>Route table:0</b> refers to <b>inet.0</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>detail extensive</b>      |
| <b>Flags</b>              | Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>detail extensive none</b> |

## Sample Output

### show interfaces extensive (Flow Monitoring)

```

user@host> show interfaces mo-4/0/0 extensive
Physical interface: mo-4/0/0, Enabled, Physical link is Up
 Interface index: 144, SNMP ifIndex: 42, Generation: 28
 Description: monitor pic 2
 Type: Adaptive-Services, Link-level type: Adaptive-Services, MTU: Unlimited,
 Clocking: Unspecified, Speed: 800mbps
 Device flags : Present Running
 Interface flags: Point-To-Point SNMP-Traps 16384
 Link type : Full-Duplex
 Link flags : None
 Physical info : Unspecified
 Hold-times : Up 0 ms, Down 0 ms
 Current address: Unspecified, Hardware address: Unspecified
 Alternate link address: Unspecified
 Last flapped : 2005-05-24 16:43:12 PDT (00:17:46 ago)
 Statistics last cleared: Never

```

## Traffic statistics:

|                 |           |             |
|-----------------|-----------|-------------|
| Input bytes :   | 756824218 | 8328536 bps |
| Output bytes :  | 872916185 | 8400160 bps |
| Input packets:  | 508452    | 697 pps     |
| Output packets: | 15577196  | 18750 pps   |

## Input errors:

Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,  
Policed discards: 0, Resource errors: 0

## Output errors:

Carrier transitions: 2, Errors: 0, Drops: 0, MTU errors: 0,  
Resource errors: 0

## Logical interface mo-4/0/0.0 (Index 83) (SNMP ifIndex 43) (Generation 26)

Flags: Point-To-Point SNMP-Traps Encapsulation: Adaptive-Services

## Traffic statistics:

|                 |           |
|-----------------|-----------|
| Input bytes :   | 756781796 |
| Output bytes :  | 872255328 |
| Input packets:  | 507233    |
| Output packets: | 15575988  |

## Local statistics:

|                 |   |
|-----------------|---|
| Input bytes :   | 0 |
| Output bytes :  | 0 |
| Input packets:  | 0 |
| Output packets: | 0 |

## Transit statistics:

|                 |           |             |
|-----------------|-----------|-------------|
| Input bytes :   | 756781796 | 8328536 bps |
| Output bytes :  | 872255328 | 8400160 bps |
| Input packets:  | 507233    | 697 pps     |
| Output packets: | 15575988  | 18750 pps   |

Protocol inet, MTU: Unlimited, Generation: 38, Route table: 0

Flags: None

## Logical interface mo-4/0/0.16383 (Index 84) (SNMP ifIndex 58) (Generation 27)

...

## show passive-monitoring error

|                                 |                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show passive-monitoring error (*   all   mo-fpc/pic/port)</code>                                                                                                                     |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                            |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Display passive monitoring error statistics.                                                                                      |
| <b>Options</b>                  | <code>*   all   mo-fpc/pic/port</code> —Display error statistics for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name.        |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">show passive-monitoring error all on page 570</a>                                                                                                                              |
| <b>Output Fields</b>            | <a href="#">Table 40 on page 569</a> lists the output fields for the <b>show passive-monitoring error</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 40: show passive-monitoring error Output Fields**

| Field Name                         | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Passive monitoring interface       | Name of the passive monitoring interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Local interface index              | Index counter of the local interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Interface state                    | State of the passive monitoring interface: <ul style="list-style-type: none"> <li>• <b>Monitoring</b>—Specified interface is actively monitoring.</li> <li>• <b>Disabled</b>—Specified interface has been disabled from the CLI.</li> <li>• <b>Not monitoring</b>—The interface is operational, but not monitoring. This condition occurs when an interface first comes online, or when the interface is operational, but no logical unit has been configured under the physical interface.</li> <li>• <b>Unknown</b>—Unknown state.</li> <li>• <b>Error</b>—An error occurred during the process of determining the state of the interface.</li> </ul> |
| <b>Error information</b>           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Packets dropped (no memory)        | Number of packets dropped because of memory shortage.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Packets dropped (not IP)           | Number of non-IP packets dropped.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Packets dropped (not IPv4)         | Number of packets dropped because they failed the IPv4 version check.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Packets dropped (header too small) | Number of packets dropped because the packet length or IP header length was too small.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Table 40: show passive-monitoring error Output Fields (*continued*)

| Field Name                        | Field Description                                                                                                                                                                             |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Memory allocation failures</b> | Number of flow record memory allocation failures. A small number reflects failures to replenish the free list. A large number indicates the monitoring station is almost out of memory space. |
| <b>Memory free failures</b>       | Number of flow record memory free failures.                                                                                                                                                   |
| <b>Memory free list failures</b>  | Number of flow records received from free list that failed. Memory is nearly exhausted or too many new flows greater than 128 KB are being created per second.                                |
| <b>Memory warning</b>             | Whether the flows have exceeded 1 million packets per second (Mpps) on a Monitoring Services PIC or 2 Mpps on a Monitoring Services II PIC. The response can be <b>Yes</b> or <b>No</b> .     |
| <b>Memory overload</b>            | Whether the memory has been overloaded. The response can be <b>Yes</b> or <b>No</b> .                                                                                                         |
| <b>PPS overload</b>               | Whether the PIC is receiving more packets per second than the configured threshold. The response can be <b>Yes</b> or <b>No</b> .                                                             |
| <b>BPS overload</b>               | Whether the PIC is receiving more bits per second than the configured threshold. The response can be <b>Yes</b> or <b>No</b> .                                                                |

## Sample Output

### show passive-monitoring error all

```

user@host> show passive-monitoring error all
Passive monitoring interface: mo-4/0/0, Local interface index: 44
Interface state: Monitoring
Error information
 Packets dropped (no memory): 0, Packets dropped (not IP): 0
 Packets dropped (not IPv4): 0, Packets dropped (header too small): 0
 Memory allocation failures: 0, Memory free failures: 0
 Memory free list failures: 0
 Memory warning: No, Memory overload: No, PPS overload: No, BPS overload: No

Passive monitoring interface: mo-4/1/0, Local interface index: 45
Interface state: Not monitoring
Error information
 Packets dropped (no memory): 0, Packets dropped (not IP): 0
 Packets dropped (not IPv4): 0, Packets dropped (header too small): 0
 Memory allocation failures: 0, Memory free failures: 0
 Memory free list failures: 0
 Memory warning: No, Memory overload: No, PPS overload: No, BPS overload: No

```

## show passive-monitoring flow

|                                 |                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show passive-monitoring flow (*   all   mo- <i>fpc/pic/port</i> )                                                                                                                         |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                           |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Display passive flow statistics.                                                                                                 |
| <b>Options</b>                  | *   all   mo- <i>fpc/pic/port</i> —Display passive flow statistics for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name.     |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                      |
| <b>List of Sample Output</b>    | <a href="#">show passive-monitoring flow all on page 572</a>                                                                                                                              |
| <b>Output Fields</b>            | <a href="#">Table 41 on page 571</a> lists the output fields for the <b>show passive-monitoring flow</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 41: show passive-monitoring flow Output Fields**

| Field Name                   | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Passive monitoring interface | Name of the passive monitoring interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Local interface index        | Index counter of the local interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Interface state              | State of the passive monitoring interface: <ul style="list-style-type: none"> <li>• <b>Monitoring</b>—Specified interface is actively monitoring.</li> <li>• <b>Disabled</b>—Specified interface has been disabled from the CLI.</li> <li>• <b>Not monitoring</b>—The interface is operational, but not monitoring. This condition occurs when an interface first comes online, or when the interface is operational, but no logical unit has been configured under the physical interface.</li> <li>• <b>Unknown</b>—Unknown state.</li> <li>• <b>Error</b>—An error occurred during the process of determining the state of the interface.</li> </ul> |
| Flow information             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Flow packets                 | Number of packets received by an operational PIC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Flow bytes                   | Number of bytes received by an operational PIC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Flow packets 10-second rate  | Number of packets per second handled by the PIC and displayed as a 10-second average.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Flow bytes 10-second rate    | Number of bytes per second handled by the PIC and displayed as a 10-second average.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Active flows                 | Number of currently active flows tracked by the PIC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Total flows                  | Total number of flows received by an operational PIC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 41: show passive-monitoring flow Output Fields (*continued*)

| Field Name                      | Field Description                                                                |
|---------------------------------|----------------------------------------------------------------------------------|
| <b>Flows exported</b>           | Total number of flows exported by an operational PIC.                            |
| <b>Flows packets exported</b>   | Total number of cflowd packets exported by an operational PIC.                   |
| <b>Flows inactive timed out</b> | Total number of flows that are exported because of inactivity.                   |
| <b>Flows active timed out</b>   | Total number of long-lived flows that are exported because of an active timeout. |

## Sample Output

### show passive-monitoring flow all

```

user@host> show passive-monitoring flow all
Passive monitoring interface: mo-4/0/0, Local interface index: 44
Interface state: Monitoring
Flow information
 Flow packets: 6533434, Flow bytes: 653343400
 Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
 Active flows: 0, Total flows: 1599
 Flows exported: 1599, Flows packets exported: 55
 Flows inactive timed out: 1599, Flows active timed out: 0

Passive monitoring interface: mo-4/1/0, Local interface index: 45
Interface state: Monitoring
Flow information
 Flow packets: 6537780, Flow bytes: 653778000
 Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
 Active flows: 0, Total flows: 1601
 Flows exported: 1601, Flows packets exported: 55
 Flows inactive timed out: 1601, Flows active timed out: 0

```

## show passive-monitoring memory

|                                 |                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show passive-monitoring memory (*   all   mo-<i>fpc/pic/port</i>)</code>                                                                                                                              |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                             |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Display passive monitoring memory and flow record statistics                                                                                       |
| <b>Options</b>                  | <code>*   all   mo-<i>fpc/pic/port</i></code> —Display memory and flow record statistics for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show passive-monitoring memory all on page 573</a>                                                                                                                                              |
| <b>Output Fields</b>            | <a href="#">Table 42 on page 573</a> lists the output fields for the <code>show passive-monitoring memory</code> command. Output fields are listed in the approximate order in which they appear.           |

**Table 42: show passive-monitoring memory Output Fields**

| Field Name                              | Field Description                                                                                                                                         |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Passive monitoring interface            | Name of the passive monitoring interface.                                                                                                                 |
| Local interface index                   | Index counter of the local interface.                                                                                                                     |
| Memory utilization                      |                                                                                                                                                           |
| Allocation count                        | Number of flow records allocated.                                                                                                                         |
| Free count                              | Number of flow records freed.                                                                                                                             |
| Maximum allocated                       | Maximum number of flow records allocated since the monitoring station booted. This number represents the peak number of flow records allocated at a time. |
| Allocations per second                  | Flow records allocated per second during the last statistics interval on the PIC.                                                                         |
| Frees per second                        | Flow records freed per second during the last statistics interval on the PIC.                                                                             |
| Total memory used,<br>Total memory free | Total memory currently used and total amount of memory currently free (in bytes).                                                                         |

## Sample Output

### show passive-monitoring memory all

```
user@host> show passive-monitoring memory all
```

```
Passive monitoring interface: mo-4/0/0, Local interface index: 44
Memory utilization
Allocation count: 1600, Free count: 1599, Maximum allocated: 1600
Allocations per second: 3200, Frees per second: 1438
Total memory used (in bytes): 103579176, Total memory free (in bytes):
163914184
```



## show passive-monitoring status

|                                 |                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show passive-monitoring status (* all mo-fpc/pic/port)</code>                                                                                                                         |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                             |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Display passive monitoring status.                                                                                                 |
| <b>Options</b>                  | <code>* all mo-fpc/pic/port</code> —Display status for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name.                       |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show passive-monitoring status all on page 576</a>                                                                                                                              |
| <b>Output Fields</b>            | <a href="#">Table 43 on page 575</a> lists the output fields for the <b>show passive-monitoring status</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 43: show passive-monitoring status Output Fields**

| Output Field                 | Output Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Passive monitoring interface | Name of the passive monitoring interface.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Local interface index        | Index counter of the local interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Interface state              | Monitoring state of the passive monitoring interface. <ul style="list-style-type: none"> <li>• <b>Monitoring</b>—PIC is actively monitoring.</li> <li>• <b>Disabled</b>—PIC has been disabled using the CLI.</li> <li>• <b>Not monitoring</b>—PIC is operational, but not monitoring. This condition can happen while the PIC is coming online, or when the PIC is operational but has no logical unit configured under the physical interface.</li> <li>• <b>Unknown</b></li> </ul> |
| Group index                  | Integer that represents the monitoring group of which the PIC is a member. <b>Group index</b> is a mapping from the group name to an index. It is not related to the number of monitoring groups.                                                                                                                                                                                                                                                                                    |
| Export interval              | Configured export interval for cflowd records, in seconds.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Export format                | Configured export format (only cflowd version 5 is supported).                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Protocol                     | Protocol the PIC is configured to monitor (only IPv4 is supported).                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Engine type                  | Configured engine type that is inserted in output cflowd packets.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Engine ID                    | Configured engine ID that is inserted in output cflowd packets.                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Sample Output

### show passive-monitoring status all

```
user@host> show passive-monitoring status all
Passive monitoring interface: mo-4/0/0, Local interface index: 44
Interface state: Monitoring
 Group index: 0
 Export interval: 15 secs, Export format: cflowd v5
 Protocol: IPv4, Engine type: 1, Engine ID: 1

Passive monitoring interface: mo-4/1/0, Local interface index: 45
Interface state: Disabled

Passive monitoring interface: mo-4/2/0, Local interface index: 46
Interface state: Not monitoring
```

## show passive-monitoring usage

|                                 |                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show passive-monitoring usage (*   all   mo-fpc/pic/port)</code>                                                                                                                           |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                  |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Display passive monitoring usage statistics.                                                                                            |
| <b>Options</b>                  | <code>*   all   mo-fpc/pic/port</code> —Display usage statistics for monitoring interfaces. Use a wildcard character, specify all interfaces, or provide a specific interface name.              |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                             |
| <b>List of Sample Output</b>    | <a href="#">show passive-monitoring usage all on page 577</a>                                                                                                                                    |
| <b>Output Fields</b>            | <a href="#">Table 44 on page 577</a> lists the output fields for the <code>show passive-monitoring usage</code> command. Output fields are listed in the approximate order in which they appear. |

**Table 44: show passive-monitoring usage Output Fields**

| Output Field                 | Output Field Description                                                                                                                                     |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Passive monitoring interface | Name of the passive monitoring interface.                                                                                                                    |
| Local interface index        | Index counter of the local interface.                                                                                                                        |
| CPU utilization              |                                                                                                                                                              |
| Uptime                       | Time, in milliseconds, that the PIC has been operational.                                                                                                    |
| Interrupt time               | Total time that the PIC has spent processing packets since the last PIC reset.                                                                               |
| Load (5 second)              | CPU load on the PIC, averaged more than 5 seconds. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time. |
| Load (1 minute)              | CPU load on the PIC, averaged more than 1 minute. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time.  |

## Sample Output

### show passive-monitoring usage all

```

user@host> show passive-monitoring usage
Passive monitoring interface: mo-4/0/0, Local interface index: 44
CPU utilization
 Uptime: 653155 milliseconds, Interrupt time: 40213754 microseconds
 Load (5 second): 20%, Load (1 minute): 17%

Passive monitoring interface: mo-4/1/0, Local interface index: 45
CPU utilization

```

Uptime: 652292 milliseconds, Interrupt time: 40223178 microseconds  
Load (5 second): 22%, Load (1 minute): 15%

Passive monitoring interface: mo-4/2/0, Local interface index: 46  
CPU utilization

Uptime: 649491 milliseconds, Interrupt time: 40173645 microseconds  
Load (5 second): 22%, Load (1 minute): 10098862%

## show services accounting aggregation

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show services accounting aggregation <i>aggregation-type</i> &lt;<i>aggregation-value</i>&gt; &lt;detail   extensive   terse&gt; &lt;limit <i>limit-value</i>&gt; &lt; name <i>service-name</i>&gt; &lt;order (bytes   packets)&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Display information about the aggregated active flows being processed by the accounting service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b><i>aggregation-type</i> &lt;<i>aggregation-value</i>&gt;</b>—Display information for a particular aggregation type and optional value:</p> <ul style="list-style-type: none"> <li><b>as &lt;<i>source-as-value</i>   <i>destination-as-value</i>   <i>input-snmp-interface-index-value</i>   <i>output-snmp-interface-index-value</i>&gt;</b>—Aggregate by autonomous system (AS).</li> <li><b>destination-prefix &lt;<i>destination-prefix-value</i>   <i>destination-as-value</i>   <i>output-snmp-interface-index-value</i>&gt;</b>—Aggregate by destination prefix.</li> <li><b>protocol-port &lt;<i>protocol-value</i>   <i>source-port-value</i>   <i>destination-port-value</i>&gt;</b>—Aggregate by protocol and port.</li> <li><b>source-destination-prefix &lt;<i>source-prefix-value</i>   <i>destination-prefix-value</i>   <i>destination-as-value</i>   <i>source-as-value</i>   <i>input-snmp-interface-index-value</i>   <i>output-snmp-interface-index-value</i>&gt;</b>—Aggregate by source and destination prefix.</li> <li><b>source-prefix &lt;<i>source-prefix-value</i>   <i>source-as-value</i>   <i>input-snmp-interface-index-value</i>&gt;</b>—Aggregate by source prefix.</li> </ul> <p><b>detail   extensive   terse</b>—(Optional) Display the specified level of output.</p> <p><b>limit <i>limit-value</i></b>—(Optional) Limit the display output to this number of flows. The default is no limit.</p> <p><b>name <i>service-name</i></b>—(Optional) Display information about the aggregated flows for a particular service name.</p> <p><b>order (bytes   packets)</b>—(Optional) Display the flow with the ordering of the highest number, either by byte count or by packet count.</p> |
| <b>Additional Information</b>   | For information about aggregation configuration options, see the <i>Junos OS Services Interfaces Library for Routing Devices</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>List of Sample Output</b>    | <a href="#">show services accounting aggregation protocol-port detail on page 581</a><br><a href="#">show services accounting aggregation source-destination-prefix on page 581</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

[show services accounting aggregation source-destination- prefix order packet detail on page 581](#)

[show services accounting aggregation source-destination- prefix extensive limit on page 582](#)

[show services accounting aggregation source-destination-prefix name terse on page 582](#)

**Output Fields** [Table 45 on page 580](#) lists the output fields for the **show services accounting aggregation** command. Output fields are listed in the approximate order in which they appear.

**Table 45: show services accounting aggregation Output Fields**

| Field Name                   | Field Description                                                                                                                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Accounting interface | Name of the service accounting interface.                                                                                                                                                                                                         |
| Local interface index        | Index corresponding to the service accounting interface.                                                                                                                                                                                          |
| Service name                 | Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, (default sampling), indicates the service was configured at the [edit forwarding-options sampling-level] hierarchy level. |
| Protocol                     | Protocol identifier and number.                                                                                                                                                                                                                   |
| Source Port                  | Source port identifier and number.                                                                                                                                                                                                                |
| Destination Port             | Destination port identifier and number.                                                                                                                                                                                                           |
| Source-AS                    | Source autonomous system (AS) number.                                                                                                                                                                                                             |
| Destination-AS               | Destination AS number.                                                                                                                                                                                                                            |
| Source Prefix                | Source prefix.                                                                                                                                                                                                                                    |
| Destination Prefix           | Destination prefix.                                                                                                                                                                                                                               |
| Source address               | Source address.                                                                                                                                                                                                                                   |
| Source prefix length         | Source prefix length.                                                                                                                                                                                                                             |
| Destination address          | Destination address.                                                                                                                                                                                                                              |
| Destination prefix length    | Destination prefix length.                                                                                                                                                                                                                        |
| Input SNMP interface index   | SNMP index of the interface the packet came in on.                                                                                                                                                                                                |
| Output SNMP interface index  | SNMP index of the interface the packet went out on.                                                                                                                                                                                               |

Table 45: show services accounting aggregation Output Fields (*continued*)

| Field Name   | Field Description                                               |
|--------------|-----------------------------------------------------------------|
| Start time   | Actual time when the packet in this aggregation was first seen. |
| End time     | Actual time when the packet in this aggregation was last seen.  |
| Flow count   | Number of flows in the aggregation.                             |
| Packet count | Number of packets in the aggregation.                           |
| Byte count   | Number of bytes in the aggregation.                             |

## Sample Output

### show services accounting aggregation protocol-port detail

```

user@host> show service accounting aggregation protocol-port detail
Service Accounting interface: mo-2/0/0, Local interface index: 468
Service name: (default sampling)
 Protocol: 6, Source port: 20, Destination port: 20
 Start time: 442349, End time: 6425714
 Flow count: 194, Packet count: 4294964388, Byte count: 4294781184

 Protocol: 0, Source port: 0, Destination port: 0
 Start time: 442349, End time: 6425749
 Flow count: 204, Packet count: 4294964324, Byte count: 4294777088

 Protocol: 17, Source port: 123, Destination port: 123
 Start time: 442364, End time: 6425784
 Flow count: 186, Packet count: 4294964152, Byte count: 4294766080

```

### show services accounting aggregation source-destination-prefix

```

user@host> show service accounting aggregation source-destination-prefix
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting
Source Destination Input Output Flow Packet
Byte prefix interface interface count count
prefix count
11.1.0.0/20 40.0.0.0/24 ge-5/0/1.0 ge-5/0/0.0 256 491761
31472704
11.1.0.0/20 40.0.1.36/32 ge-5/0/1.0 ge-5/0/0.0 1
1926 123264
11.1.0.0/20 40.0.1.59/32 ge-5/0/1.0 ge-5/0/0.0 1
1926 123264
11.1.0.0/20 40.0.3.63/32 ge-5/0/1.0 ge-5/0/0.0 1
1925 123200
11.1.0.0/20 40.0.3.32/32 ge-5/0/1.0 ge-5/0/0.0 1
1925

```

### show services accounting aggregation source-destination- prefix order packet detail

```

user@host> show service accounting aggregation source-destination-prefix order packet detail
name t2 input-snmp-interface-index 538

```

```

Service Accounting interface: mo-2/0/0, Local interface index: 468
Service name: t2
Source Destination Input SNMP Output SNMP Flow Packet Byte
Prefix Prefix Index Index Count Count Count
11.1.1.2/20 30.0.167.1/0 538 432 1 60 46483
11.1.1.2/20 30.0.168.1/0 538 432 1 60 5191
11.1.1.2/20 30.0.154.1/0 538 432 2 60 45504
11.1.1.2/20 30.0.76.1/0 538 432 1 60 42177
11.1.1.2/20 30.0.149.1/0 538 432 1 60 49184
11.1.1.2/20 30.0.113.1/0 538 432 2 60 48757

```

#### show services accounting aggregation source-destination- prefix extensive limit

```

user@host> show service accounting aggregation source-destination-prefix name t2 extensive
limit 3

```

```

Service Accounting interface: mo-2/0/0, Local interface index: 542
Service name: t2

```

```

Source address: 11.1.1.2, Source prefix length: 20
Destination address: 44.200.176.1, Destination prefix length: 0
Input SNMP interface index: 24, Output SNMP interface index: 26
Source-AS: 69, Destination-AS: 69
Start time: Fri Feb 21 14:16:57 2003, End time: Fri Feb 21 14:22:50 2003
Flow count: 0, Packet count: 6, Byte count: 5340

```

```

Source address: 11.1.1.2, Source prefix length: 20
Destination address: 45.243.160.1, Destination prefix length: 0
Input SNMP interface index: 24, Output SNMP interface index: 26
Source-AS: 69, Destination-AS: 69
Start time: Fri Feb 21 14:16:57 2003, End time: Fri Feb 21 14:22:50 2003
Flow count: 0, Packet count: 6, Byte count: 5490

```

```

Source address: 11.1.1.2, Source prefix length: 20
Destination address: 45.162.160.1, Destination prefix length: 0
Input SNMP interface index: 24, Output SNMP interface index: 26
Source-AS: 69, Destination-AS: 69
Start time: Fri Feb 21 14:16:57 2003, End time: Fri Feb 21 14:22:50 2003
Flow count: 0, Packet count: 6, Byte count: 4079

```

#### show services accounting aggregation source-destination-prefix name terse

```

user@host> show service accounting aggregation source-destination-prefix name T3 terse

```

```

Service Accounting interface: rsp0, Local interface index: 171

```

```

Service name: T3

```

```

Interface state: Accounting

```

| Source      | Destination  | Input      | Output     | Flow  | Packet |
|-------------|--------------|------------|------------|-------|--------|
| Byte        |              |            |            |       |        |
| prefix      | prefix       | interface  | interface  | count | count  |
| 11.1.0.0/20 | 50.0.0.0/24  | ge-5/0/1.0 | ge-5/0/0.0 | 256   | 639822 |
| 40948608    |              |            |            |       |        |
| 11.1.0.0/20 | 50.0.2.67/32 | ge-5/0/1.0 | ge-5/0/0.0 | 1     |        |
| 2485        | 159040       |            |            |       |        |
| 11.1.0.0/20 | 50.0.2.92/32 | ge-5/0/1.0 | ge-5/0/0.0 | 1     |        |
| 2485        |              |            |            |       |        |



## show services accounting aggregation template

|                                 |                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show services accounting aggregation template</b><br><b>&lt;template-name <i>template-name</i>&gt;</b>                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 8.3.                                                                                                                                                                |
| <b>Description</b>              | Display information for flow aggregation version 9 templates.                                                                                                                                              |
| <b>Options</b>                  | <b>&lt;template-name <i>template-name</i>&gt;</b> —(Optional) Display information for the specified template only.                                                                                         |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">show services accounting aggregation template on page 583</a>                                                                                                                                  |
| <b>Output Fields</b>            | <a href="#">Table 46 on page 583</a> lists the output fields for the <b>show services accounting aggregation template</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 46: show services accounting aggregation template Output Fields**

| Field Name                    | Field Description               |
|-------------------------------|---------------------------------|
| <b>MPLS Label 1</b>           | Position of first MPLS label.   |
| <b>MPLS Label 2</b>           | Position of second MPLS label.  |
| <b>MPLS Label 3</b>           | Position of third MPLS label.   |
| <b>MPLS Top Level Address</b> | Outer top label FEC IP address. |
| <b>Packet Count</b>           | Number of packets sent.         |

## Sample Output

### show services accounting aggregation template

```

user@host> show services accounting aggregation template template-name mpls
MPLS label 1: 299808, MPLS label 2: 0, MPLS label 3: 0
Source address: 11.1.1.2, Destination address: 10.255.15.22, Top Label Address:
22.15.255.10
Source port: 0, Destination port: 0
Protocol: 61, TOS: 0, TCP flags: 0
Source mask: 24, Destination mask: 32
Input SNMP interface index: 503, Output SNMP interface index: 505
Start time: 40780, End time: 157330
Packet count: 3949198, Byte count: 181663062

```

## show services accounting errors

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show services accounting errors</code><br><code>&lt;inline-jflow   name (*   all   service-name)&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Display active flow error statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>none</b>—Display error statistics for all services accounting instances.</p> <p><b>inline-jflow fpc-slot slot-number</b>—(Optional) Display error statistics for inline jflow.</p> <p><b>name (*   all   service-name)</b>—(Optional) Display active flow error statistics. Use a wildcard character, specify all services, or provide a specific service name.</p>                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">show services accounting flow on page 588</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>List of Sample Output</b>    | <p><a href="#">show services accounting errors (Monitoring PIC interface) on page 585</a></p> <p><a href="#">show services accounting errors (Service PIC interface) on page 586</a></p> <p><a href="#">show services accounting errors inline-jflow fpc-slot slot-number (when only IPv6 is configured) on page 586</a></p> <p><a href="#">show services accounting errors inline-jflow fpc-slot slot-number (when both IPv4 and IPv6 are configured) on page 586</a></p> <p><a href="#">show services accounting errors inline-jflow (MX80 Router when both IPv4 and IPv6 are configured) on page 586</a></p> |
| <b>Output Fields</b>            | <a href="#">Table 47 on page 584</a> lists the output fields for the <b>show services accounting errors</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                    |

Table 47: show services accounting errors Output Fields

| Field                        | Field Description                                                                                                                                                                                                                                                       |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Accounting interface | Name of the service accounting interface.                                                                                                                                                                                                                               |
| Local interface index        | Index counter of the local interface.                                                                                                                                                                                                                                   |
| FPC slot                     | Slot number of the FPC for which the flow information is displayed. (Available only when the <b>inline-jflow fpc-slot slot-number</b> option is used.)                                                                                                                  |
| Service name                 | Name of a service that was configured at the <b>[edit forwarding-options accounting]</b> hierarchy level. The default display, <b>(default sampling)</b> , indicates the service was configured at the <b>[edit forwarding-options sampling-level]</b> hierarchy level. |

### Error Information

Table 47: show services accounting errors Output Fields (*continued*)

| Field                              | Field Description                                                                                                                                                                             |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packets dropped (no memory)        | Number of packets dropped because of memory shortage.                                                                                                                                         |
| Packets dropped (not IP)           | Number of non-IP packets dropped.                                                                                                                                                             |
| Packets dropped (not IPv4)         | Number of packets dropped because they failed the IPv4 version check.                                                                                                                         |
| Packets dropped (header too small) | Number of packets dropped because the packet length or IP header length was too small.                                                                                                        |
| Memory allocation failures         | Number of flow record memory allocation failures. A small number reflects failures to replenish the free list. A large number indicates the monitoring station is almost out of memory space. |
| Memory free failures               | Number of flow record memory free failures.                                                                                                                                                   |
| Memory free list failures          | Number of flow records received from the free list that failed. Memory is nearly exhausted, or too many new flows greater than 128 KB are being created per second.                           |
| Memory overload                    | Whether the memory has been overloaded. The response can be <b>Yes</b> or <b>No</b> .                                                                                                         |
| PPS overload                       | Whether the PIC is receiving more packets per second than the configured threshold. The response can be <b>Yes</b> or <b>No</b> .                                                             |
| BPS overload                       | Whether the PIC is receiving more bits per second than the configured threshold. The response can be <b>Yes</b> or <b>No</b> .                                                                |
| Flow Creation Failures             | Number of times flow creation failed.                                                                                                                                                         |
| Route Record Lookup Failures       | Number of times the route record lookup failed.                                                                                                                                               |
| AS Lookup Failures                 | Number of times autonomous system lookup failed.                                                                                                                                              |
| Export Packet Failures             | Number of times packet export failed.                                                                                                                                                         |

## Sample Output

### show services accounting errors (Monitoring PIC interface)

```

user@host> show services accounting errors
Service Accounting interface: mo-1/1/0, Local interface index: 15
Service name: (default sampling)
Error information
 Packets dropped (no memory): 0, Packets dropped (not IP): 0
 Packets dropped (not IPv4): 0, Packets dropped (header too small): 0
 Memory allocation failures: 0, Memory free failures: 0
 Memory free list failures: 0
 Memory overload: No, PPS overload: No, BPS overload: No

```

## Sample Output

### show services accounting errors (Service PIC interface)

```
user@host> show services accounting errors
Service Accounting interface: sp-0/1/0
Service name: (default sampling)
Error information
 Service sets dropped: 0, Active timeout failures: 0
 Export packet failures: 0, Flow creation failures: 0
 Memory overload: No

Service Accounting interface: sp-1/0/0
Service name: (default sampling)
Error information
 Service sets dropped: 0, Active timeout failures: 0
 Export packet failures: 0, Flow creation failures: 0
 Memory overload: No
```

### show services accounting errors inline-jflow fpc-slot slot-number (when only IPv6 is configured)

```
user@host> show services accounting errors inline-jflow fpc-slot 5
Error information
 FPC Slot: 5
 Flow Creation Failures: 0
 Route Record Lookup Failures: 0, AS Lookup Failures: 0
 Export Packet Failures: 0
 Memory Overload: No, Memory Alloc Fail Count: 0
```

### show services accounting errors inline-jflow fpc-slot slot-number (when both IPv4 and IPv6 are configured)

```
user@host> show services accounting errors inline-jflow fpc-slot 5
Error information
 FPC Slot: 5
 Flow Creation Failures: 0
 Route Record Lookup Failures: 0, AS Lookup Failures: 0
 Export Packet Failures: 0
 Memory Overload: No, Memory Alloc Fail Count: 0

IPv4:
 IPv4 Flow Creation Failures: 0
 IPv4 Route Record Lookup Failures: 0, IPv4 AS Lookup Failures: 0
 IPv4 Export Packet Failures: 0

IPv6:
 IPv6 Flow Creation Failures: 0
 IPv6 Route Record Lookup Failures: 0, IPv6 AS Lookup Failures: 0
 IPv6 Export Packet Failures: 0
```

### show services accounting errors inline-jflow (MX80 Router when both IPv4 and IPv6 are configured)

```
user@host> show services accounting errors inline-jflow
Error information
 TFEB Slot: 0
 Flow Creation Failures: 0
 Route Record Lookup Failures: 0, AS Lookup Failures: 0
 Export Packet Failures: 0
 Memory Overload: No

IPv4:
 IPv4 Flow Creation Failures: 0
```

IPv4 Route Record Lookup Failures: 0, IPv4 AS Lookup Failures: 0  
IPv4 Export Packet Failures: 0

IPv6:

IPv6 Flow Creation Failures: 0  
IPv6 Route Record Lookup Failures: 0, IPv6 AS Lookup Failures: 0  
IPv6 Export Packet Failures: 0

## show services accounting flow

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show services accounting flow</code><br><code>&lt;inline-jflow   logical-system   name (*   all   service-name)&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br>Junos OS Release 10.0 added the capability to display output from multiple sampling instances.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Display active flow statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b>none</b>—Display active flow statistics for all service instances.</p> <p><b>logical-system (all   logical-system)</b>—(Optional) Display active flow statistics for the specified logical system or all logical systems on the device.</p> <p><b>inline-jflow (fpc-slot slot-number)</b>—(Optional) Display inline flow statistics for the specified FPC.</p> <p><b>name (*   all   service-name)</b>—(Optional) Display services accounting active flow statistics. Use a wildcard character, specify all services, or provide a specific service name.</p>                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">show services accounting status on page 602</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>List of Sample Output</b>    | <a href="#">show services accounting flow (flow aggregation v5/v8 configuration) on page 589</a><br><a href="#">show services accounting flow (flow aggregation v9 configuration) on page 589</a><br><a href="#">show services accounting flow name on page 590</a><br><a href="#">show services accounting flow name all on page 590</a><br><a href="#">show services accounting flow (multiple sampling instances) on page 591</a><br><a href="#">show services accounting flow inline-jflow fpc-slot slot-number (for IPv4 flow) on page 591</a><br><a href="#">show services accounting flow inline-jflow fpc-slot slot-number (with IPv4 and IPv6 Configuration) on page 591</a><br><a href="#">show services accounting flow inline-jflow (MX80 Router with IPv4 and IPv6 Configuration) on page 591</a> |
| <b>Output Fields</b>            | <a href="#">Table 48 on page 588</a> lists the output fields for the <b>show services accounting flow</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Table 48: show services accounting flow Output Fields**

| Output Field                 | Output Field Description                  |
|------------------------------|-------------------------------------------|
| Service Accounting interface | Name of the service accounting interface. |
| Local interface index        | Index counter of the local interface.     |

Table 48: show services accounting flow Output Fields (*continued*)

| Output Field                       | Output Field Description                                                                                                                                                                                                                                   |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Service name</b>                | Name of a service that was configured at the [edit forwarding-options accounting] hierarchy level. The default display, ( <b>default sampling</b> ), indicates the service was configured at the [edit forwarding-options sampling-level] hierarchy level. |
| <b>Flow Information</b>            |                                                                                                                                                                                                                                                            |
| <b>FPC Slot</b>                    | Slot number of the FPC for which the flow information is displayed. (Available only when the inline-jflow fpc-slot slot-number option is used.)                                                                                                            |
| <b>Flow packets</b>                | Number of packets received by an operational PIC.                                                                                                                                                                                                          |
| <b>Flow bytes</b>                  | Number of bytes received by an operational PIC.                                                                                                                                                                                                            |
| <b>Flow packets 10-second rate</b> | Number of packets per second handled by the PIC and displayed as a 10-second average.                                                                                                                                                                      |
| <b>Flow bytes 10-second rate</b>   | Number of bytes per second handled by the PIC and displayed as a 10-second average.                                                                                                                                                                        |
| <b>Active flows</b>                | Number of currently active flows tracked by the PIC.                                                                                                                                                                                                       |
| <b>Total flows</b>                 | Total number of flows received by an operational PIC.                                                                                                                                                                                                      |
| <b>Flows exported</b>              | Total number of flows exported by an operational PIC.                                                                                                                                                                                                      |
| <b>Flows packets exported</b>      | Total number of cflowd packets exported by an operational PIC.                                                                                                                                                                                             |
| <b>Flows inactive timed out</b>    | Total number of flows that are exported because of inactivity.                                                                                                                                                                                             |
| <b>Flows active timed out</b>      | Total number of long-lived flows that are exported because of an active timeout.                                                                                                                                                                           |

## Sample Output

### show services accounting flow (flow aggregation v5/v8 configuration)

```

user@host> show services accounting flow
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting
Flow information
 Flow packets: 87168293, Flow bytes: 5578770752
 Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928962
 Active flows: 1000, Total flows: 2000
 Flows exported: 19960, Flows packets exported: 582
 Flows inactive timed out: 1000, Flows active timed out: 29000

```

### show services accounting flow (flow aggregation v9 configuration)

```

user@host> show services accounting flow
Flow information
 Service Accounting interface: sp-7/1/0, Local interface index: 149

```

```
Flow packets: 0, Flow bytes: 0
Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
Active flows: 0, Total flows: 0
Flows exported: 0, Flows packets exported: 1
Flows inactive timed out: 0, Flows active timed out: 0
```

#### show services accounting flow name

```
user@host> show services accounting flow count2
Service Accounting interface: mo-1/1/0, Local interface index: 15
Service name: count2
Flow information
Flow packets: 0, Flow bytes: 0
Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
Active flows: 0, Total flows: 0
Flows exported: 0, Flows packets exported: 0
Flows inactive timed out: 0, Flows active timed out: 0
```

#### show services accounting flow name all

```
user@host> show services accounting flow name all
Service Accounting interface: rsp0, Local interface index: 171
Service name: T2
Interface state: Accounting
Flow information
Flow packets: 37609891, Flow bytes: 2407033024
Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928953
Active flows: 1000, Total flows: 1000
Flows exported: 6705, Flows packets exported: 198
Flows inactive timed out: 0, Flows active timed out: 13000

Service Accounting interface: rsp0, Local interface index: 171
Service name: T3
Interface state: Accounting
Flow information
Flow packets: 37750807, Flow bytes: 2416051712
Flow packets 10-second rate: 45762, Flow bytes 10-second rate: 2928940
Active flows: 1000, Total flows: 1000
Flows exported: 13437, Flows packets exported: 378
Flows inactive timed out: 0, Flows active timed out: 13000

Service Accounting interface: rsp0, Local interface index: 171
Service name: T4
Interface state: Accounting
Flow information
Flow packets: 0, Flow bytes: 0
Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
Active flows: 0, Total flows: 0
Flows exported: 0, Flows packets exported: 0
Flows inactive timed out: 0, Flows active timed out: 0

Service Accounting interface: rsp0, Local interface index: 171
Service name: count1
Interface state: Accounting
Flow information
Flow packets: 0, Flow bytes: 0
Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
Active flows: 0, Total flows: 0
Flows exported: 0, Flows packets exported: 0
Flows inactive timed out: 0, Flows active timed out: 0
```



**show services accounting flow (multiple sampling instances)**

```

user@host> show services accounting flow
Flow information
Service Accounting interface: sp-2/0/0, Local interface index: 215
Flow packets: 9867, Flow bytes: 631488
Flow packets 10-second rate: 0, Flow bytes 10-second rate: 628
Active flows: 2, Total flows: 10
Flows exported: 4028, Flows packets exported: 6150
Flows inactive timed out: 8, Flows active timed out: 4026

Service Accounting interface: sp-2/1/0, Local interface index: 223
Flow packets: 0, Flow bytes: 0
Flow packets 10-second rate: 0, Flow bytes 10-second rate: 0
Active flows: 0, Total flows: 0
Flows exported: 0, Flows packets exported: 1
Flows inactive timed out: 0, Flows active timed out: 0

```

**show services accounting flow inline-jflow fpc-slot slot-number (for IPv4 flow)**

```

user@host> show services accounting flow inline-jflow fpc-slot 5
Flow information
FPC Slot: 5
Flow Packets: 0, Flow Bytes: 0
Active Flows: 0, Total Flows: 0
Flows Exported: 0, Flow Packets Exported: 0
Flows Inactive Timed Out: 0, Flows Active Timed Out: 0

```

**show services accounting flow inline-jflow fpc-slot slot-number (with IPv4 and IPv6 Configuration)**

```

user@host> show services accounting flow inline-jflow fpc-slot 5
Flow information
FPC Slot: 5
Flow Packets: 0, Flow Bytes: 0
Active Flows: 0, Total Flows: 0
Flows Exported: 0, Flow Packets Exported: 0
Flows Inactive Timed Out: 0, Flows Active Timed Out: 0

IPv4 Flows:
IPv4 Flow Packets: 0, IPv4 Flow Bytes: 0
IPv4 Active Flows: 0, IPv4 Total Flows: 0
IPv4 Flows Exported: 0, IPv4 Flow Packets exported: 0
IPv4 Flows Inactive Timed Out: 0, IPv4 Flows Active Timed Out: 0

IPv6 Flows:
IPv6 Flow Packets: 0, IPv6 Flow Bytes: 0
IPv6 Active Flows: 0, IPv6 Total Flows: 0
IPv6 Flows Exported: 0, IPv6 Flow Packets Exported: 0
IPv6 Flows Inactive Timed Out: 0, IPv6 Flows Active Timed Out: 0

```

**show services accounting flow inline-jflow (MX80 Router with IPv4 and IPv6 Configuration)**

```

user@host> show services accounting flow inline-jflow
Flow information
TFEB Slot: 0
Flow Packets: 0, Flow Bytes: 0
Active Flows: 0, Total Flows: 0
Flows Exported: 0, Flow Packets Exported: 0
Flows Inactive Timed Out: 0, Flows Active Timed Out: 0

IPv4 Flows:

```

IPv4 Flow Packets: 0, IPv4 Flow Bytes: 0  
IPv4 Active Flows: 0, IPv4 Total Flows: 0  
IPv4 Flows Exported: 0, IPv4 Flow Packets exported: 0  
IPv4 Flows Inactive Timed Out: 0, IPv4 Flows Active Timed Out: 0

IPv6 Flows:  
IPv6 Flow Packets: 0, IPv6 Flow Bytes: 0  
IPv6 Active Flows: 0, IPv6 Total Flows: 0  
IPv6 Flows Exported: 0, IPv6 Flow Packets Exported: 0  
IPv6 Flows Inactive Timed Out: 0, IPv6 Flows Active Timed Out: 0

## show services accounting flow-detail

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                 | <pre>show services accounting flow-detail &lt;detail   extensive   terse&gt; &lt;filters&gt; &lt;limit <i>limit-value</i>&gt; &lt;name (*   all   <i>service-name</i>)&gt; &lt;order (bytes   packets)&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>    | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>            | Display information about the flows being processed by the accounting service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                | <p><b>detail   extensive   terse</b>—(Optional) Display the specified level of output.</p> <p><b>filters</b>—(Optional) Filter the display output of the currently active flow records. The following filters query actively changing data structures and result in different results for multiple invocations:</p> <ul style="list-style-type: none"> <li>• <b>destination-as</b>—Display flow records filtered by destination autonomous system information.</li> <li>• <b>destination-port</b>—Display flow records filtered by destination port information.</li> <li>• <b>destination-prefix</b>—Display flow records filtered by destination prefix information.</li> <li>• <b>input-snmp-interface-index</b>—Display flow records filtered by SNMP input interface index information.</li> <li>• <b>output-snmp-interface-index</b>—Display flow records filtered by SNMP output interface index information.</li> <li>• <b>proto</b>—Display flow records filtered by protocol type.</li> <li>• <b>source-as</b>—Display flow records filtered by source autonomous system information.</li> <li>• <b>source-port</b>—Display flow records filtered by source port information.</li> <li>• <b>source-prefix</b>—Display flow records filtered by source prefix information.</li> <li>• <b>tos</b>—Display flow records filtered by type of service classification.</li> </ul> <p><b>limit <i>limit-value</i></b>—(Optional) Limit the display output to the specified number of flows. The default is no limit.</p> <p><b>name (*   all   <i>service-name</i>)</b>—(Optional) Display information about the flows being processed. Use a wildcard character, specify all services, or provide a specific services name.</p> <p><b>order (bytes   packets)</b>—(Optional) Display the flow with the ordering of the highest number, either by byte count or by packet count.</p> |
| <b>Additional Information</b> | When no PIC is active, or when no route record has been downloaded from the PIC, this command reports no flows, even though packets are being sampled. This command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

displays information about two concurrent sessions only. If a third session is attempted, the command pauses with no output until one of the previous sessions is completed.

**Required Privilege Level** view

**List of Sample Output** [show services accounting flow-detail on page 595](#)  
[show services accounting flow-detail limit on page 596](#)  
[show services accounting flow-detail name extensive on page 596](#)  
[show services accounting flow-detail limit order bytes on page 596](#)  
[show services accounting flow-detail source-port on page 597](#)

**Output Fields** [Table 49 on page 594](#) lists the output fields for the **show services accounting flow-detail** command. Output fields are listed in the approximate order in which they appear.

**Table 49: show services accounting flow-detail Output Fields**

| Field Name                          | Field Description                                                                                                                                                                                                                                                 | Output Level     |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <b>Service Accounting interface</b> | Name of the service accounting interface.                                                                                                                                                                                                                         | All levels       |
| <b>Service name</b>                 | Name of a service that was configured at the <b>[edit forwarding-options accounting]</b> hierarchy level. The default display, <b>(default sampling)</b> , indicates the service was configured at the <b>[edit forwarding-options sampling]</b> hierarchy level. | All levels       |
| <b>Local interface index</b>        | Index counter of the local interface.                                                                                                                                                                                                                             | All levels       |
| <b>TOS</b>                          | Type-of-service value from the IP header.                                                                                                                                                                                                                         | <b>extensive</b> |
| <b>Input SNMP interface index</b>   | SNMP index of the interface on which the packet came in.                                                                                                                                                                                                          | <b>extensive</b> |
| <b>Output SNMP interface index</b>  | SNMP index of the interface on which the packet went out.                                                                                                                                                                                                         | <b>extensive</b> |
| <b>Source-AS</b>                    | Source AS number.                                                                                                                                                                                                                                                 | <b>extensive</b> |
| <b>Destination-AS</b>               | Destination AS number.                                                                                                                                                                                                                                            | <b>extensive</b> |
| <b>Protocol</b>                     | Name of the protocol used for the packet flow from the corresponding source address.                                                                                                                                                                              | All levels       |
| <b>Input interface</b>              | Interface on which the packets were received.                                                                                                                                                                                                                     | All levels       |
| <b>Output interface</b>             | Interface on which the packets were transmitted.                                                                                                                                                                                                                  | All levels       |
| <b>TCP flags</b>                    | Number of TCP header flags detected in the flow.                                                                                                                                                                                                                  | <b>extensive</b> |
| <b>Source address</b>               | Address where the flow originated.                                                                                                                                                                                                                                | All levels       |
| <b>Source port</b>                  | Name of the source port.                                                                                                                                                                                                                                          | All levels       |

Table 49: show services accounting flow-detail Output Fields (*continued*)

| Field Name                           | Field Description                                                                     | Output Level     |
|--------------------------------------|---------------------------------------------------------------------------------------|------------------|
| Source prefix length                 | Source prefix length.                                                                 | extensive        |
| Destination address                  | Address where the flow is sent.                                                       | All levels       |
| Destination prefix length            | Destination prefix length.                                                            | extensive        |
| Destination port                     | Name of the destination port.                                                         | All levels       |
| Start time                           | Actual time when the packet in this aggregation was first seen.                       | detail extensive |
| End time                             | Actual time when the packet in this aggregation was last seen.                        | detail extensive |
| Packet count                         | Number of packets in the aggregation.                                                 | All levels       |
| Byte count                           | Number of bytes in the aggregation.                                                   | All levels       |
| Time since last active timeout       | Amount of time elapsed since the last active timeout, in the format <i>hh:mm:ss</i> . | None specified   |
| Packet count for last active timeout | Number of packets in the aggregation since the last active timeout.                   | None specified   |
| Byte count for last active timeout   | Number of bytes in the aggregation since the last active timeout.                     | None specified   |

## Sample Output

### show services accounting flow-detail

In this sample, the output is split into three sections, with ellipses (...) indicating where the sections are continued.

```

user@host> show services accounting flow-detail
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting
Protocol Input Source Source Output
 interface address port interface...
tcp(6) ge-5/0/1.0 11.1.1.2 0 ge-5/0/0.0
tcp(6) ge-5/0/1.0 11.1.1.2 0 ge-5/0/0.0

Destination Destination Packet Byte Time since last
address port count count active timeout...
40.0.3.149 0 2660 170240 00:00:58
40.0.3.138 0 2660 170240 00:00:58

Packet count for Byte count for
last active timeout last active timeout
2805 179520
2805 179520

```

**show services accounting flow-detail limit**

In this sample, the output is split into three sections, with ellipses (...) indicating where the sections are continued.

```

user@host> show services accounting flow-detail limit 1
Service Accounting interface: rsp0, Local interface index: 171
Service name: (default sampling)
Interface state: Accounting

```

| Protocol | Input interface | Source address | Source port | Output interface... |
|----------|-----------------|----------------|-------------|---------------------|
| tcp(6)   | ge-5/0/1.0      | 11.1.1.2       | 0           | ge-5/0/0.0          |

| Destination address | Destination port | Packet count | Byte count | Time since last active timeout... |
|---------------------|------------------|--------------|------------|-----------------------------------|
| 40.0.3.149          | 0                | 2158         | 138112     | 00:00:47                          |

```

Packet count for Byte count for
last active timeout last active timeout
 2827 180928

```

**show services accounting flow-detail name extensive**

```

user@host> show services accounting flow-detail name cf-2 extensive
Service Accounting interface: mo-0/2/0, Local interface index: 145
Service name: cf-2
 TOS: 0, Protocol: udp(17), TCP flags: 0
 Source address: 10.10.10.1, Source prefix length: 0, Destination address:
20.20.20.20,
 Destination prefix length: 0, Source port: 1173, Destination port: 69
 Input SNMP interface index: 65, Output SNMP interface index: 0, Source-AS: 0,
 Destination-AS: 0
 Start time: 62425, End time: 635265, Packet count: 165845, Byte count: 9453165

```

**show services accounting flow-detail limit order bytes**

The output of the following command is displayed over 141 columns, not the standard 80 columns. In this sample, the output is split into three sections, with ellipses (...) indicating where the sections are continued.

```

user@host> show services accounting flow-detail limit 5 order bytes
Service Accounting interface: mo-2/0/0, Local interface index: 356
Service name: (default sampling)

```

| Protocol | Input interface | Source address | Source port | Output interface... |
|----------|-----------------|----------------|-------------|---------------------|
| icmp(1)  | ge-2/3/0.0      | 11.1.1.2       | 0           | .local.             |
| icmp(1)  | ge-2/3/0.0      | 11.1.1.2       | 0           | .local.             |
| icmp(1)  | ge-2/3/0.0      | 11.1.1.2       | 0           | .local.             |
| icmp(1)  | ge-2/3/0.0      | 11.1.1.2       | 0           | .local.             |
| icmp(1)  | ge-2/3/0.0      | 11.1.1.2       | 0           | .local.             |

| Destination address | Destination port | Packet count | Byte count | Time since last active timeout... |
|---------------------|------------------|--------------|------------|-----------------------------------|
| 51.88.128.2         | 0                | 16           | 12148      | Not applicable                    |
| 52.78.144.2         | 0                | 16           | 15229      | Not applicable                    |
| 51.147.192.2        | 0                | 16           | 13296      | Not applicable                    |
| 51.136.16.2         | 0                | 16           | 13924      | Not applicable                    |
| 50.214.48.2         | 0                | 16           | 13428      | Not applicable                    |

```

Packet count for Byte count for

```

|                     |                     |
|---------------------|---------------------|
| last active timeout | last active timeout |
| Not applicable      | Not applicable      |
| Not applicable      | Not applicable      |
| Not applicable      | Not applicable      |
| Not applicable      | Not applicable      |
| Not applicable      | Not applicable      |

#### show services accounting flow-detail source-port

```
user@host> show services accounting flow-detail name cf-2 detail source-port 1173
Service Accounting interface: mo-0/2/0, Local interface index: 145
Service name: cf-2
 Protocol: udp(17), Source address: 10.10.10.1, Source port: 1173, Destination
address:
20.20.20.20, Destination port: 69
 Start time: 62425, End time: 811115, Packet count: 142438, Byte count: 8118966
```

## show services accounting memory

|                                 |                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services accounting memory                                                                                                                                               |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                               |
| <b>Description</b>              | Display memory and flow record statistics.                                                                                                                                    |
| <b>Options</b>                  | This command has no options.                                                                                                                                                  |
| <b>Required Privilege Level</b> | view                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">show services accounting memory (Monitoring PIC interface) on page 598</a><br><a href="#">show services accounting memory (Service PIC interface) on page 599</a> |
| <b>Output Fields</b>            | Table 50 on page 598 lists the output fields for the <b>show services accounting memory</b> command. Output fields are listed in the approximate order in which they appear.  |

Table 50: show services accounting memory Output Fields

| Output Field                 | Output Field Description                                                                                                                                  |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Accounting interface | Name of the service accounting interface.                                                                                                                 |
| Memory Utilization           |                                                                                                                                                           |
| Local interface index        | Index counter of the local interface.                                                                                                                     |
| Allocation count             | Number of flow records allocated.                                                                                                                         |
| Free count                   | Number of flow records freed.                                                                                                                             |
| Maximum allocated            | Maximum number of flow records allocated since the monitoring station booted. This number represents the peak number of flow records allocated at a time. |
| Allocations per second       | Flow records allocated per second during the last statistics interval on the PIC.                                                                         |
| Frees per second             | Flow records freed per second during the last statistics interval on the PIC.                                                                             |
| Total memory used            | Total amount of memory currently used (in bytes).                                                                                                         |
| Total memory free            | Total amount of memory currently free (in bytes).                                                                                                         |

## Sample Output

### show services accounting memory (Monitoring PIC interface)

```

user@host> show services accounting memory
Service Accounting interface: mo-2/0/0, Local interface index: 468
Memory utilization

```



```
Allocation count: 437340, Free count: 433699, Maximum allocated: 6782
Allocations per second: 3366, Frees per second: 6412
Total memory used (in bytes): 133460320,
Total memory free (in bytes): 133918352
```

## Sample Output

### show services accounting memory (Service PIC interface)

```
user@host> show services accounting memory
Service Accounting interface: sp-0/1/0
Memory utilization
 Allocation count: 1000, Free count: 0
 Allocations per second: 0, Frees per second: 0
 Total memory used (in bytes): 218158272
 Total memory free (in bytes): 587147696

Service Accounting interface: sp-1/0/0
Memory utilization
 Allocation count: 1000, Free count: 0
 Allocations per second: 0, Frees per second: 0
 Total memory used (in bytes): 218157592
 Total memory free (in bytes): 587148376
```

## show services accounting packet-size-distribution

|                                 |                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services accounting packet-size-distribution<br><name (*   all   <i>service-name</i> )>                                                                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                              |
| <b>Description</b>              | Display a packet size distribution histogram.                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b>none</b>—Display a packet size distribution histogram of all accounting services.</p> <p><b>name (*   all   <i>service-name</i>)</b>—(Optional) Display a packet size distribution histogram. Use a wildcard character, specify all services, or provide a specific services name.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                         |
| <b>List of Sample Output</b>    | <a href="#">show services accounting packet-size-distribution name on page 600</a>                                                                                                                                                                                                           |
| <b>Output Fields</b>            | <a href="#">Table 51 on page 600</a> lists the output fields for the <b>show services accounting packet-size-distribution</b> command. Output fields are listed in the approximate order in which they appear.                                                                               |

Table 51: show services accounting packet-size-distribution Output Fields

| Field Name                   | Field Description                                                                                                                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Accounting interface | Name of the service accounting interface.                                                                                                                                                                                                         |
| Service name                 | Name of a service that was configured at the [edit-forwarding-options accounting] hierarchy level. The default display, (default sampling), indicates the service was configured at the [edit-forwarding-options sampling-level] hierarchy level. |
| Local interface index        | Index counter of the local interface.                                                                                                                                                                                                             |
| Range start                  | Smallest packet length (in bytes) to count.                                                                                                                                                                                                       |
| Range end                    | Largest packet length (in bytes) to count.                                                                                                                                                                                                        |
| Number of packets            | Count of packets detected in the size between Range start and Range end.                                                                                                                                                                          |
| Percentage packets           | Percentage of the total number of packets that are in this size range.                                                                                                                                                                            |

## Sample Output

### show services accounting packet-size-distribution name

```
user@host> show services accounting packet-size-distribution name test3
Service Accounting interface: mo-0/2/0, Local interface index: 163
Service name: test3
```

|             |           |                   |                    |
|-------------|-----------|-------------------|--------------------|
| Range start | Range end | Number of packets | Percentage packets |
| 32          | 64        | 2924              | 100                |

## show services accounting status

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show services accounting status</code><br><code>&lt;inline-jflow fpc-slot <i>slot-number</i>   name (*   all   <i>service-name</i>)&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 13.2R2 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Display available Physical Interface Cards (PICs) for accounting services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b>none</b>—Display available PICs for all accounting services.</p> <p><b>inline-jflow fpc-slot <i>slot-number</i></b>—(Optional) Display inline flow accounting status for the specified FPC. For a two-member MX Series Virtual Chassis or EX9200 Virtual Chassis, the master router or switch uses FPC slot numbers 0 through 11 with no offset; the backup router or switch uses FPC slot numbers 12 through 23, with an offset of 12.</p> <p><b>name (*   all   <i>service-name</i>)</b>—(Optional) Display available PICs. Use a wildcard character, specify all services, or provide a specific services name.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">show services accounting flow on page 588</a></li> <li><a href="#">Inline Flow Monitoring for Virtual Chassis Overview</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>List of Sample Output</b>    | <p><a href="#">show services accounting status name (Monitoring PIC interface) on page 603</a></p> <p><a href="#">show services accounting status name (Service PIC interface) on page 603</a></p> <p><a href="#">show services accounting status inline-jflow fpc-slot (when both IPv4 and IPv6 are configured) on page 604</a></p> <p><a href="#">show services accounting status inline-jflow (MX80 Router when both IPv4 and IPv6 are configured) on page 604</a></p>                                                                                                                                                    |
| <b>Output Fields</b>            | <a href="#">Table 52 on page 602</a> lists the output fields for the <b>show services accounting status</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Table 52: show services accounting status Output Fields**

| Field                        | Field Description                                                                                                                                                                                                                                                                         |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Accounting interface | Name of the service accounting interface.                                                                                                                                                                                                                                                 |
| Service name                 | Name of a service that was configured at the <code>[edit-forwarding-options accounting]</code> hierarchy level. The default display, <code>(default sampling)</code> , indicates the service was configured at the <code>[edit-forwarding-options sampling-level]</code> hierarchy level. |
| FPC Slot                     | Slot number of the FPC for which the flow information is displayed.                                                                                                                                                                                                                       |

Table 52: show services accounting status Output Fields (*continued*)

| Field                        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local interface index        | Index counter of the local interface.                                                                                                                                                                                                                                                                                                                                                                                                           |
| Interface state              | Accounting state of the passive monitoring interface. <ul style="list-style-type: none"> <li>• <b>Accounting</b>—PIC is actively accounting.</li> <li>• <b>Disabled</b>—PIC has been disabled from the CLI.</li> <li>• <b>Not accounting</b>—PIC is up but not accounting. This can happen while the PIC is coming online, or when the PIC is up but has no logical unit configured under the physical interface.</li> <li>• Unknown</li> </ul> |
| Group index                  | Integer that represents the monitoring group of which the PIC is a member. <b>Group index</b> is a mapping from the group name to an index. It is not related to the number of monitoring groups.                                                                                                                                                                                                                                               |
| Export interval (in seconds) | Configured export interval for cflowd records, in seconds.                                                                                                                                                                                                                                                                                                                                                                                      |
| Export format                | Configured export format.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Protocol                     | Protocol the PIC is configured to monitor.                                                                                                                                                                                                                                                                                                                                                                                                      |
| Engine type                  | Configured engine type that is inserted in output cflowd packets.                                                                                                                                                                                                                                                                                                                                                                               |
| Engine ID                    | Configured engine ID that is inserted in output cflowd packets.                                                                                                                                                                                                                                                                                                                                                                                 |
| Route Record Count           | Number of routes recorded.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| AS Record Count              | Number of autonomous systems recorded.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Route Records Set            | Status of route recording; whether routes are recorded or not.                                                                                                                                                                                                                                                                                                                                                                                  |
| Configuration Set            | Status of monitoring configuration; whether monitoring configuration is set or not.                                                                                                                                                                                                                                                                                                                                                             |

## Sample Output

### show services accounting status name (Monitoring PIC interface)

```

user@host> show services accounting status name count1
Service Accounting interface: mo-2/0/0, Local interface index: 468
Service name: count1
Interface state: Accounting
 Group index: 0
 Export interval (in seconds): 60, Export format: cflowd v8
 Protocol: IPv4, Engine type: 55, Engine ID: 5

```

## Sample Output

### show services accounting status name (Service PIC interface)

```

user@host> show services accounting status name

```

```
Service Accounting interface: sp-0/1/0
Interface state: Accounting
 Export format: 9, Route record count: 0
 IFL to SNMP index count: 7, AS count: 0
 Configuration set: Yes, Route record set: No, IFL SNMP map set: Yes

Service Accounting interface: sp-1/0/0
Interface state: Accounting
 Export format: 9, Route record count: 33
 IFL to SNMP index count: 7, AS count: 1
 Configuration set: Yes, Route record set: Yes, IFL SNMP map set: Yes
```

#### show services accounting status inline-jflow fpc-slot (when both IPv4 and IPv6 are configured)

```
user@host> show services accounting status inline-jflow fpc-slot 5
FPC Slot: 5
 IPv4 export format: Version-IPFIX, IPv6 export format: Version-IPFIX
 VPLS export format: Not set
 IPv4 Route Record Count: 5, IPv6 Route Record Count: 7
 Route Record Count: 12, AS Record Count: 1
 Route-Records Set: Yes, Config Set: Yes
```

#### show services accounting status inline-jflow (MX80 Router when both IPv4 and IPv6 are configured)

```
user@host> show services accounting status inline-jflow

Status information
 TFEB Slot: 0
 Export format: IP-FIX
 IPv4 Route Record Count: 6, IPv6 Route Record Count: 8
 Route Record Count: 14, AS Record Count: 1
 Route-Records Set: Yes, Config Set: Yes
```

## show services accounting usage

|                                 |                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services accounting usage<br><name <i>service-name</i> >                                                                                                               |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                             |
| <b>Description</b>              | Display the CPU usage of PIC used for active flow monitoring.                                                                                                               |
| <b>Options</b>                  | <p><b>none</b>—Display CPU usage for all service names.</p> <p><b>name <i>service-name</i></b>—(Optional) Display CPU usage for the specified service name.</p>             |
| <b>Additional Information</b>   | When no route record has been downloaded from the PIC, this command reports no flows, even though packets are being sampled.                                                |
| <b>Required Privilege Level</b> | view                                                                                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show services accounting usage (Monitoring PIC interface) on page 606</a><br><a href="#">show services accounting usage (Service PIC interface) on page 606</a> |
| <b>Output Fields</b>            | Table 53 on page 605 lists the output fields for the <b>show services accounting usage</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 53: show services accounting usage Output Fields**

| Output Field                 | Output Field Description                                                                                                                                                                                                                                   |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Accounting interface | Name of the service accounting interface.                                                                                                                                                                                                                  |
| Service name                 | Name of a service that was configured at the [edit-forwarding-options accounting] hierarchy level. The default display, ( <b>default sampling</b> ), indicates the service was configured at the [edit-forwarding-options sampling-level] hierarchy level. |
| Local interface index        | Index counter of the local interface.                                                                                                                                                                                                                      |
| Uptime                       | Time that the PIC has been operational (in milliseconds).                                                                                                                                                                                                  |
| Interrupt time               | Total time that the PIC has spent processing packets since the last PIC reset (in microseconds).                                                                                                                                                           |
| Load (5 second)              | CPU load on the PIC, averaged more than 5 seconds. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time.                                                                                               |
| Load (1 minute)              | CPU load on the PIC, averaged more than 1 minute. The number is a percentage obtained by dividing the time spent on active tasks by the total elapsed time.                                                                                                |

## Sample Output

### show services accounting usage (Monitoring PIC interface)

```
user@host> show services accounting usage
Service Accounting interface: mo-1/1/0, Local interface index: 15
Service name: (default sampling)
CPU utilization
 Uptime: 600413856 milliseconds, Interrupt time: 2403 microseconds
 Load (5 second): 43%, Load (1 minute): 24%
```

## Sample Output

### show services accounting usage (Service PIC interface)

```
user@host> show services accounting usage
Service Accounting interface: sp-0/1/0
Service name: (default sampling)
CPU utilization
 Uptime: 7853940 milliseconds, Interrupt time: 0 microseconds
 Load (5 second): 2%, Load (1 minute): 0%

Service Accounting interface: sp-0/1/0
Service name: (default sampling)
CPU utilization
 Uptime: 331160 milliseconds, Interrupt time: 0 microseconds
 Load (5 second): 2%, Load (1 minute): 0%
```



## show services dynamic-flow-capture content-destination

|                                 |                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services dynamic-flow-capture content-destination capture-group <i>group-name</i><br>destination-identifier <i>identifier</i><br><terse>                                                                              |
| <b>Release Information</b>      | Command introduced in Junos OS Release 7.4.                                                                                                                                                                                |
| <b>Description</b>              | (M320 routers and T Series routers only) Display information about the content destination that receives packets from the dynamic flow capture (DFC) interface.                                                            |
| <b>Options</b>                  | <p><b>capture-group <i>group-name</i></b>—Capture-group identifier.</p> <p><b>destination-identifier <i>identifier</i></b>—Content destination identifier.</p> <p><b>terse</b>—(Optional) Display summary information.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">show services dynamic-flow-capture content-destination on page 608</a>                                                                                                                                         |
| <b>Output Fields</b>            | <a href="#">Table 54 on page 607</a> lists the output fields for the <b>show services dynamic-flow-capture content-destination</b> command. Output fields are listed in the approximate order in which they appear.        |

**Table 54: show services dynamic-flow-capture content-destination Output Fields**

| Output Field                    | Output Field Description                                   | Level of Output |
|---------------------------------|------------------------------------------------------------|-----------------|
| <b>Capture group</b>            | Name of the capture group.                                 | to be provided  |
| <b>Content destination</b>      | Name of the content destination.                           | to be provided  |
| <b>Criteria</b>                 | Number of criteria specified.                              | to be provided  |
| <b>Bandwidth</b>                | Bandwidth used by the matched traffic.                     | to be provided  |
| <b>Matched packets</b>          | Number of matched packets sent to the content destination. | to be provided  |
| <b>Matched bytes</b>            | Number of matched bytes sent to the content destination.   | to be provided  |
| <b>Congestion notifications</b> | Number of notification messages sent.                      | to be provided  |

## Sample Output

### show services dynamic-flow-capture content-destination

```
user@host> show services dynamic-flow-capture content-destination capture-group g1
destination-identifier cd1 terse
 Capture group: g1, Content destination: cd1, Criteria: 0, Bandwidth: 0, Matched
 packets: 0, Matched bytes: 0, Congestion notifications: 0
```

## show services dynamic-flow-capture control-source

|                                 |                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show services dynamic-flow-capture control-source capture-group <i>group-name</i> control-source <i>identifier</i> &lt;detail   terse&gt;</code>                                                                                             |
| <b>Release Information</b>      | Command introduced in Junos OS Release 7.4.                                                                                                                                                                                                        |
| <b>Description</b>              | (M320 routers and T Series routers only) Display information about the control source that makes dynamic flow capture requests to the dynamic flow capture interface.                                                                              |
| <b>Options</b>                  | <p><code>capture-group <i>group-name</i></code>—Capture group identifier.</p> <p><code>control-source <i>identifier</i></code>—Control source identifier.</p> <p><code>detail   terse</code>—(Optional) Display the specified level of output.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                               |
| <b>List of Sample Output</b>    | <a href="#">show services dynamic-flow-capture control-source on page 610</a><br><a href="#">show services dynamic-flow-capture control-source detail on page 610</a>                                                                              |
| <b>Output Fields</b>            | Table 55 on page 609 lists the output fields for the <code>show services dynamic-flow-capture control-source</code> command. Output fields are listed in the approximate order in which they appear.                                               |

**Table 55: show services dynamic-flow-capture control-source Output Fields**

| Output Field                        | Output Field Description                                                                                                 |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Capture group                       | Name of the capture group.                                                                                               |
| Control source                      | Name of the control source.                                                                                              |
| Criteria added, Criteria add failed | Number of criteria added or added and failed.                                                                            |
| Active criteria                     | Number of active criteria.                                                                                               |
| Static criteria, Dynamic criteria   | Number of static or dynamic criteria.                                                                                    |
| Control protocol requests           | Total number of control protocol requests.                                                                               |
| Requests                            | Number of <b>Add</b> , <b>Delete</b> , <b>List</b> , <b>Refresh</b> , and <b>No-op</b> control protocol requests.        |
| Failed                              | Number of <b>Add</b> , <b>Delete</b> , <b>List</b> , <b>Refresh</b> , and <b>No-op</b> failed control protocol requests. |
| Add request rate                    | Rate of add requests.                                                                                                    |

Table 55: show services dynamic-flow-capture control-source Output Fields (*continued*)

| Output Field                  | Output Field Description                                                                                                                                                                                                 |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add request peak rate         | Peak rate of add requests.                                                                                                                                                                                               |
| Bandwidth across all criteria | Bandwidth used by all the requests.                                                                                                                                                                                      |
| Total notifications           | Total number of notifications sent and the number of notifications by category: <b>Restart</b> , <b>Rollover</b> , <b>Timeout</b> , <b>Congestion</b> , <b>Congestion delete</b> , and <b>Dups</b> (duplicates) dropped. |
| Criteria deleted              | Total number of criteria deleted and the number of deleted criteria by category: <b>Timeout idle</b> , <b>Timeout total</b> , <b>Packets</b> , and <b>Bytes</b> .                                                        |
| Sequence number               | Sequence number.                                                                                                                                                                                                         |

## Sample Output

### show services dynamic-flow-capture control-source

```

user@host> show services dynamic-flow-capture control-source source-identifier cs0_cg0
capture-group cg_0
Capture group: cg_0, Control source: cs0_cg0
Criteria added: 28, Criteria add failed: 0, Active criteria: 0, Control protocol
requests: 28, Add request rate: 0,
Add request peak rate: 1, Bandwidth across all criteria: 0, Total notifications:
1, Criteria deleted: 28, Sequence number: 0

```

### show services dynamic-flow-capture control-source detail

```

user@host> show services dynamic-flow-capture control-source source-identifier cs0_cg0
capture-group cg_0 detail
Capture group: cg_0, Control source: cs0_cg0
Criteria added: 28, Criteria add failed: 0
Active criteria: 0
Static criteria: 0, Dynamic criteria: 0
Control protocol requests: 28

```

|          | Add | Delete | List | Refresh | No-op |
|----------|-----|--------|------|---------|-------|
| Requests | 28  | 0      | 0    | 0       | 0     |
| Failed   | 0   | 0      | 0    | 0       | 0     |

```

Add request rate: 0
Add request peak rate: 1
Bandwidth across all criteria: 0
Total notifications: 1
Restart: 1, Rollover: 0, No-op: 0, Timeout: 0, Congestion: 0, Congestion
delete: 0, Dups dropped: 0
Criteria deleted: 28
Timeout idle: 0, Timeout total: 0, Packets: 0, Bytes: 0
Sequence number: 0

```

## show services dynamic-flow-capture statistics

|                                 |                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services dynamic-flow-capture statistics capture-group <i>group-name</i>                                                                                                                              |
| <b>Release Information</b>      | Command introduced in Junos OS Release 7.4.                                                                                                                                                                |
| <b>Description</b>              | (M320 routers and T Series routers only) Display statistics information about the capture group specified for dynamic flow capture.                                                                        |
| <b>Options</b>                  | capture-group <i>group-name</i> —Capture group identifier.                                                                                                                                                 |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">show services dynamic-flow-capture statistics on page 612</a>                                                                                                                                  |
| <b>Output Fields</b>            | <a href="#">Table 56 on page 611</a> lists the output fields for the <b>show services dynamic-flow-capture statistics</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 56: show services dynamic-flow-capture statistics Output Fields**

| Output Field           | Output Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Input                  | <p>Incoming dynamic flow capture packet statistics:</p> <ul style="list-style-type: none"> <li>• <b>Control protocol packets</b>—Number of control protocol packets received.</li> <li>• <b>Captured data packets</b>—Number of data packets captured.</li> <li>• <b>Control IRI packets</b>—Number of control IRI packets received.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Control protocol drops | <p>Control protocol packets dropped for the following reasons:</p> <ul style="list-style-type: none"> <li>• <b>Not IP packets</b>—Dropped packets were not IP packets.</li> <li>• <b>Not UDP packets</b>—Dropped packets were not User Datagram Protocol (UDP) packets.</li> <li>• <b>Invalid destination address</b>—Dropped packets had invalid destination addresses.</li> <li>• <b>No memory</b>—Packets dropped because of insufficient memory.</li> <li>• <b>Unauthorized control source</b>—Packets dropped because the control source was not authenticated.</li> <li>• <b>Bad request</b>—Packets dropped because the request was invalid.</li> <li>• <b>Unknown control source</b>—Packets dropped because the control source was not known.</li> <li>• <b>Not DTCP</b>—Dropped packets did not adhere to the control protocol format.</li> <li>• <b>Bad command line</b>—Packets dropped because of a version mismatch.</li> <li>• <b>Bandwidth exceeded</b>—Packets dropped because the bandwidth was exceeded.</li> <li>• <b>Drop rate due to exceeded bandwidth</b>—Rate of traffic dropped because the bandwidth was exceeded.</li> <li>• <b>Other</b>—Packets dropped for other reasons or undetermined causes.</li> </ul> |

Table 56: show services dynamic-flow-capture statistics Output Fields (*continued*)

| Output Field           | Output Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input drops</b>     | <p>Incoming dynamic flow capture packets dropped for the following reasons:</p> <ul style="list-style-type: none"> <li>• <b>Unknown packets</b>—Packets dropped because the packet type was not recognized.</li> <li>• <b>Captured data not IPv4</b>—Packets dropped because they were not IPv4 packets.</li> <li>• <b>Captured data too small</b>—Packets dropped because they were smaller than the size reported in their headers.</li> <li>• <b>Captured data drops</b>—Data packets dropped because of undetermined causes.</li> <li>• <b>Captured data not matched</b>—Packets dropped because they did not match filter criteria.</li> <li>• <b>Bandwidth exceeded</b>—Packets dropped because the bandwidth was exceeded.</li> <li>• <b>Drop rate due to exceeded bandwidth</b>—Rate of traffic dropped because the bandwidth was exceeded.</li> </ul> |
| <b>Output</b>          | <p>Outgoing dynamic flow capture packet statistics:</p> <ul style="list-style-type: none"> <li>• <b>Control protocol packets</b>—Number of control protocol packets sent.</li> <li>• <b>Captured data packets</b>—Number of captured data packets sent.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Output drops</b>    | <p>Outgoing packets dropped:</p> <ul style="list-style-type: none"> <li>• <b>Control protocol drops</b>—Number of control protocol packets dropped.</li> <li>• <b>Captured data drops</b>—Number of captured data packets dropped.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Flow Statistics</b> | <p>DFC flow statistics:</p> <ul style="list-style-type: none"> <li>• <b>Active flow cache entries</b></li> <li>• <b>Active flow cache usage percentage</b></li> <li>• <b>Flow cache entries allocated</b></li> <li>• <b>Number of control sources</b></li> <li>• <b>Number of content destinations</b></li> <li>• <b>Number of criteria</b></li> <li>• <b>Maximum criteria matching one flow</b></li> <li>• <b>Cached flows purged for memory</b></li> <li>• <b>Maximum filters matching one packet</b></li> </ul>                                                                                                                                                                                                                                                                                                                                             |

## Sample Output

### show services dynamic-flow-capture statistics

```

user@host> show services dynamic-flow-capture statistics capture-group g1
Input:

Control protocol packets: 643, Captured data packets: 69977, Control IRI packets:
337

Control protocol drops:

Not IP packets: 0, Not UDP packets: 3, Invalid destination address: 0, No memory:
0, Unauthorized control source: 0,

Bad request: 0, Unknown control source: 0, Not DTCP: 0, Bad command line: 0,
Bandwidth exceeded: 0,

```

Drop rate due to exceeded bandwidth: 0, Other: 0

Input drops:

Unknown packets: 0, Captured data not IPv4: 0, Captured data too small: 0,  
Captured data drops: 0, Captured data not matched: 0,

Bandwidth exceeded: 0, Drop rate due to exceeded bandwidth: 0

Output:

Control protocol packets: 644, Captured data packets: 1119624

Output drops:

Control protocol drops: 0, Captured data drops: 0

Flow Statistics:

Active flow cache entries: 40, Active flow cache usage percentage: 0, Flow cache  
entries allocated: 40,

Number of control sources: 4, Number of content destinations: 64, Number of  
criteria: 640,

Maximum criteria matching one flow: 16, Cached flows purged for memory: 0,  
Maximum filters matching one packet: 16

## show services flow-collector file interface

|                                 |                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services flow-collector file interface (all   cp-fpc/pic/port)<br><detail   extensive   terse>                                                                                                                                  |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                      |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Display information about flow collector files.                                                                                                                             |
| <b>Options</b>                  | <p><b>all   cp-fpc/pic/port</b>—Display file information for all configured flow collector interfaces or for the specified interface.</p> <p><b>detail   extensive   terse</b>—(Optional) Display the specified level of output.</p> |
| <b>Additional Information</b>   | No entries are displayed for files that have been successfully transferred.                                                                                                                                                          |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                 |
| <b>List of Sample Output</b>    | <a href="#">show services flow-collector file interface extensive on page 615</a>                                                                                                                                                    |
| <b>Output Fields</b>            | <a href="#">Table 57 on page 614</a> lists the output fields for the <b>show services flow-collector file interface</b> command. Output fields are listed in the approximate order in which they appear.                             |

Table 57: show services flow-collector file interface Output Fields

| Output Field      | Output Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Level of Output  |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <b>Filename</b>   | Name of the file created on the flow collector interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | All levels       |
| <b>Flows</b>      | Total number of collector flows for which records are present in the file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | none specified   |
| <b>Throughput</b> | Throughput statistics: <ul style="list-style-type: none"> <li>• <b>Flow records</b>—Number of flow records in the file.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of flow records per second.</li> <li>• <b>peak per second</b>—Peak number of flow records per second.</li> </ul> </li> <li>• <b>Uncompressed bytes</b>—Total file size before compression.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of uncompressed bytes per second.</li> <li>• <b>peak per second</b>—Peak number of uncompressed bytes per second.</li> </ul> </li> <li>• <b>Compressed bytes</b>—Total file size after compression.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of compressed bytes per second.</li> <li>• <b>peak per second</b>—Peak number of compressed bytes per second.</li> </ul> </li> </ul> | <b>extensive</b> |



Table 57: show services flow-collector file interface Output Fields (*continued*)

| Output Field | Output Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Level of Output |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Status       | <p>File statistics:</p> <ul style="list-style-type: none"> <li>• <b>Compressed blocks</b>—(extensive output only) Data blocks in the file that have been compressed. The file is exported only when the compressed block count and block count become the same.</li> <li>• <b>Block count</b>—(extensive output only) Total number of data blocks in the file.</li> <li>• <b>State</b>—Processing state of the file. <ul style="list-style-type: none"> <li>• <b>Active</b>—The flow collector interface is writing to the file.</li> <li>• <b>Export 1</b>—File export is in progress to the primary server.</li> <li>• <b>Export 2</b>—File export is in progress to the secondary server.</li> <li>• <b>Wait</b>—File is pending export.</li> </ul> </li> <li>• <b>Transfer attempts 0</b>—Number of attempts made to transfer the file. If the file is successfully transferred in the first attempt, this field is 0.</li> </ul> | All levels      |

## Sample Output

### show services flow-collector file interface extensive

```

user@host> show services flow-collector file interface cp-3/2/0 extensive
Filename: cFlowd-py69Ni69-0-20031112_014301-so_3_0_0_0.bcp.bi.gz
Throughput:
 Flow records: 188365, per second: 238, peak per second: 287
 Uncompressed bytes: 21267756, per second: 27007, peak per second: 32526
 Compressed bytes: 2965643, per second: 0, peak per second: 22999
Status:
 Compressed blocks: 156, Block count: 156
 State: Active, Transfer attempts: 0

```

## show services flow-collector input interface

|                                 |                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show services flow-collector input interface (all   <i>cp-fpc/pic/port</i>)</code><br><code>&lt;detail   extensive   terse&gt;</code>                                                                                          |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                      |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Display the number of packets received by collector interfaces from monitoring interfaces.                                                                                  |
| <b>Options</b>                  | <b>all   <i>cp-fpc/pic/port</i></b> —Display packets received by all configured flow collector interfaces or by the specified interface.<br><br><b>detail   extensive   terse</b> —(Optional) Display the specified level of output. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                 |
| <b>List of Sample Output</b>    | <a href="#">show services flow-collector input interface on page 616</a><br><a href="#">show services flow-collector input interface all on page 616</a>                                                                             |
| <b>Output Fields</b>            | <a href="#">Table 58 on page 616</a> lists the output fields for the <b>show services flow-collector input interface</b> command. Output fields are listed in the approximate order in which they appear.                            |

**Table 58: show services flow-collector input interface Output Fields**

| Output Field     | Output Field Description                                                                   |
|------------------|--------------------------------------------------------------------------------------------|
| <b>Interface</b> | Name of the monitoring interface.                                                          |
| <b>Packets</b>   | Number of packets traveling from the monitoring interface to the flow collector interface. |
| <b>Bytes</b>     | Number of bytes traveling from the monitoring interface to the flow collector interface.   |

## Sample Output

### show services flow-collector input interface

```
user@host> show services flow-collector input interface cp-3/2/0
Interface Packets Bytes
mo-3/0/0.0 21706 32328568
mo-3/1/0.0 21706 32329096
```

### show services flow-collector input interface all

```
user@host> show services flow-collector input interface all
Flow collector interface: cp-6/1/0
Interface state: Collecting flows
Interface Packets Bytes
mo-3/0/0.0 274 416232
mo-3/3/0.0 274 416184
```

|            |     |        |
|------------|-----|--------|
| mo-1/0/0.0 | 274 | 416232 |
| mo-1/1/0.0 | 274 | 416232 |
| mo-1/2/0.0 | 274 | 416232 |
| mo-1/3/0.0 | 274 | 416232 |
| mo-3/1/0.0 | 274 | 416232 |
| mo-4/0/0.0 | 274 | 416232 |
| mo-4/1/0.0 | 274 | 416232 |
| mo-4/2/0.0 | 274 | 416184 |
| mo-4/3/0.0 | 274 | 416232 |
| mo-5/0/0.0 | 274 | 416232 |
| mo-5/1/0.0 | 274 | 416232 |
| mo-5/2/0.0 | 274 | 416232 |
| mo-5/3/0.0 | 274 | 416232 |
| mo-6/0/0.0 | 274 | 416232 |

Flow collector interface: cp-6/3/0  
Interface state: Collecting flows

## show services flow-collector interface

|                                 |                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services flow-collector interface (all   <i>cp-fpc/pic/port</i> )<br><detail   extensive   terse>                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | (M40e, M160, and M320 routers and T Series routers only) Display overall statistics for the flow collector application.                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>all   <i>cp-fpc/pic/port</i></b>—Display statistics for flow collector applications on all interfaces or for the specified interface.</p> <p><b>detail   extensive   terse</b>—(Optional) Display the specified level of output.</p>                                                                                        |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                              |
| <b>List of Sample Output</b>    | <a href="#">show services flow-collector interface all detail on page 620</a><br><a href="#">show services flow-collector interface all extensive on page 621</a><br><a href="#">show services flow-collector interface all terse on page 623</a><br><a href="#">show services flow-collector interface extensive on page 623</a> |
| <b>Output Fields</b>            | Table 59 on page 618 lists the output fields for the <b>show services flow-collector interface</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                               |

Table 59: show services flow-collector interface Output Fields

| Output Field             | Output Field Description                                                                      | Level of Output  |
|--------------------------|-----------------------------------------------------------------------------------------------|------------------|
| Flow collector interface | Name of the flow collector interface.                                                         | All levels       |
| Interface state          | Collecting flow state for the interface.                                                      | All levels       |
| Packets                  | Total number of packets received.                                                             | none specified   |
| Flows Uncompressed Bytes | Total uncompressed data size for all files created on this PIC.                               | none specified   |
| Compressed Bytes         | Total compressed data size for all files created on this PIC.                                 | none specified   |
| FTP bytes                | Total number of bytes transferred to the FTP server, including those dropped during transfer. | none specified   |
| FTP files                | Total number of FTP transfers attempted by the server.                                        | none specified   |
| Memory                   | Bytes used on the PIC and bytes free.                                                         | detail extensive |

Table 59: show services flow-collector interface Output Fields (*continued*)

| Output Field      | Output Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Level of Output         |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <b>Input</b>      | Incoming flow collector packet statistics: <ul style="list-style-type: none"> <li>• <b>Packets</b>—Number of packets received on the unit.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of packets per second.</li> <li>• <b>peak per second</b>—Peak number of packets per second.</li> </ul> </li> <li>• <b>Bytes</b>—Number of bytes received on the unit.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of bytes per second.</li> <li>• <b>peak per second</b>—Peak number of bytes per second.</li> </ul> </li> <li>• <b>Flow records processed</b>—Number of records in the flow collector packets that were processed by the flow-collector interface.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of flow records processed per second.</li> <li>• <b>peak per second</b>—Peak number of flow records per second.</li> </ul> </li> </ul>                                                                 | <b>detail extensive</b> |
| <b>Allocation</b> | Data block statistics: <ul style="list-style-type: none"> <li>• <b>Blocks allocated</b>—Total number of data blocks (containing flow records) allocated to the files created on this PIC.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of blocks allocated per second.</li> <li>• <b>peak per second</b>—Peak number of blocks allocated per second.</li> </ul> </li> <li>• <b>Blocks freed</b>—Total number of data blocks freed.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of blocks freed per second.</li> <li>• <b>peak per second</b>—Peak number of blocks freed per second.</li> </ul> </li> <li>• <b>Blocks unavailable</b>—Total number of data block requests denied, typically because of a memory shortage.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of blocks unavailable per second.</li> <li>• <b>peak per second</b>—Peak number of blocks unavailable per second.</li> </ul> </li> </ul> | <b>extensive</b>        |
| <b>Files</b>      | File statistics, incremented since the PIC last booted: <ul style="list-style-type: none"> <li>• <b>Files created</b>—Total number of files created on this PIC.</li> <li>• <b>Files exported</b>— Number of files successfully created and exported.</li> <li>• <b>Files destroyed</b>— (<b>extensive</b> output only) Number of files successfully exported and files dropped by the flow collection interface.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>detail extensive</b> |
| <b>Throughput</b> | Throughput statistics: <ul style="list-style-type: none"> <li>• <b>Uncompressed bytes</b>—Total uncompressed data size for all files created on this PIC.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of uncompressed bytes per second.</li> <li>• <b>peak per second</b>—Peak number of uncompressed bytes per second.</li> </ul> </li> <li>• <b>Compressed bytes</b>—Total compressed data size for all files created on this PIC.               <ul style="list-style-type: none"> <li>• <b>per second</b>—Average number of compressed bytes per second.</li> <li>• <b>peak per second</b>—Peak number of compressed bytes per second.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                     | <b>detail extensive</b> |

Table 59: show services flow-collector interface Output Fields (*continued*)

| Output Field                    | Output Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Level of Output         |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <b>Packet drops</b>             | <p>Number of packets dropped for the following causes:</p> <ul style="list-style-type: none"> <li>• <b>No memory</b>—Packets dropped because of insufficient memory.</li> <li>• <b>Not IP</b>—Packets dropped because they are not IP packets.</li> <li>• <b>Not IPv4</b>—Packets dropped because they are not IP version 4 packets.</li> <li>• <b>Too small</b>—Packets dropped because each packet was smaller than the size reported in its header.</li> <li>• <b>Fragments</b>—Packets dropped because of fragmentation. Fragments are not reassembled.</li> <li>• <b>ICMP</b>—Packets dropped because they are not ICMP packets.</li> <li>• <b>TCP</b>—Packets dropped because they are not TCP packets.</li> <li>• <b>Unknown</b>—Packets dropped because of undetermined causes.</li> <li>• <b>Not Junos flow</b>—Packets dropped because they are not interpreted by Junos OS. Junos OS interprets only IPv4, UDP cflowd version 5 packets.</li> </ul>                                                                                                                                                                                                                                                                                                                         | <b>extensive</b>        |
| <b>File transfer</b>            | <p>File transfer statistics:</p> <ul style="list-style-type: none"> <li>• <b>FTP bytes</b>—Total number of bytes transferred to the FTP server, including those dropped during transfer.</li> <li>• <b>FTP files</b>—Total number of FTP transfers attempted by the server.</li> <li>• <b>FTP failure</b>—Total number of FTP failures encountered by the server.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>detail extensive</b> |
| <b>Flow collector interface</b> | Physical interface acting as a flow collector.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>detail</b>           |
| <b>Export channel</b>           | <p>Export channel 0 is unit 0. Export channel 1 is unit 1. Flow receive channel is unit 2. Server status statistics are the following:</p> <ul style="list-style-type: none"> <li>• <b>Current server Primary or Secondary</b>—Current FTP server being used. Value is</li> <li>• <b>Primary server state</b>—State of the server: <ul style="list-style-type: none"> <li>• <b>OK</b>—Server is operating without problems.</li> <li>• <b>FTP error</b>—Server encountered an FTP protocol error while sending files.</li> <li>• <b>Network error</b>—Flow-collector interface has errors when contacting the primary FTP server.</li> <li>• <b>Unknown</b>—First file transfer has not been sent to the primary server.</li> </ul> </li> <li>• <b>Secondary server state</b>—State of the server: <ul style="list-style-type: none"> <li>• <b>OK</b>—Server is operating without errors.</li> <li>• <b>FTP error</b>—Server encountered an FTP protocol error while sending files.</li> <li>• <b>Network error</b>—Flow-collector interface has errors when contacting the secondary FTP server.</li> <li>• <b>Unknown</b>—First file transfer has not been sent to the secondary server.</li> </ul> </li> <li>• <b>Not configured</b>—Secondary server is not configured.</li> </ul> | <b>detail extensive</b> |

## Sample Output

### show services flow-collector interface all detail

```
user@host> show services flow-collector interface all detail
```

```

Flow collector interface: cp-6/1/0
Interface state: Collecting flows
Memory:
 Used: 51452732, Free: 440329088
Input:
 Packets: 4384, per second: 0, peak per second: 156
 Bytes: 6659616, per second: 0, peak per second: 249695
 Flow records processed: 131070, per second: 0, peak per second: 4914
Files:
 Files created: 1, per second: 0, peak per second: 0
 Files exported: 1, per second: 0, peak per second: 0
Throughput:
 Uncompressed bytes: 13742307, per second: 0, peak per second: 593564
 Compressed bytes: 3786177, per second: 0, peak per second: 162826
File Transfer:
 FTP bytes: 3786247, per second: 0, peak per second: 378620
 FTP files: 1, per second: 0, peak per second: 0
 FTP failure: 0
Export channel: 0
 Current server: Primary
 Primary server state: OK, Secondary server state: OK
Export channel: 1
 Current server: Primary
 Primary server state: Unknown, Secondary server state: OK

Flow collector interface: cp-6/3/0
Interface state: Collecting flows
Memory:
 Used: 51452732, Free: 440329088
Input:
 Packets: 0, per second: 0, peak per second: 0
 Bytes: 0, per second: 0, peak per second: 0
 Flow records processed: 0, per second: 0, peak per second: 0
Files:
 Files created: 0, per second: 0, peak per second: 0
 Files exported: 0, per second: 0, peak per second: 0
Throughput:
 Uncompressed bytes: 0, per second: 0, peak per second: 0
 Compressed bytes: 0, per second: 0, peak per second: 0
File Transfer:
 FTP bytes: 70, per second: 0, peak per second: 6
 FTP files: 0, per second: 0, peak per second: 0
 FTP failure: 0
Export channel: 0
 Current server: Primary
 Primary server state: Unknown, Secondary server state: OK
Export channel: 1
 Current server: Primary
 Primary server state: Unknown, Secondary server state: OK

```

#### show services flow-collector interface all extensive

```

user@host> show services flow-collector interface all extensive
Flow collector interface: cp-6/1/0
Interface state: Collecting flows
Memory:
 Used: 51452732, Free: 440329088
Input:
 Packets: 4384, per second: 0, peak per second: 156
 Bytes: 6659616, per second: 0, peak per second: 249695
 Flow records processed: 131070, per second: 0, peak per second: 4914

```

Allocation:  
Blocks allocated: 108, per second: 0, peak per second: 0  
Blocks freed: 108, per second: 0, peak per second: 10  
Blocks unavailable: 0, per second: 0, peak per second: 0

Files:  
Files created: 1, per second: 0, peak per second: 0  
Files exported: 1, per second: 0, peak per second: 0  
Files destroyed: 1, per second: 0, peak per second: 0

Throughput:  
Uncompressed bytes: 13742307, per second: 0, peak per second: 593564  
Compressed bytes: 3786177, per second: 0, peak per second: 162826

Packet drops:  
No memory: 0, Not IP: 0  
Not IPv4: 0, Too small: 0  
Fragments: 0, ICMP: 0  
TCP: 0, Unknown: 0  
Not JUNOS flow: 0

File Transfer:  
FTP bytes: 3786247, per second: 0, peak per second: 378620  
FTP files: 1, per second: 0, peak per second: 0  
FTP failure: 0

Export channel: 0  
Current server: Primary  
Primary server state: OK, Secondary server state: OK

Export channel: 1  
Current server: Primary  
Primary server state: Unknown, Secondary server state: OK

Flow collector interface: cp-6/3/0  
Interface state: Collecting flows

Memory:  
Used: 51452732, Free: 440329088

Input:  
Packets: 0, per second: 0, peak per second: 0  
Bytes: 0, per second: 0, peak per second: 0  
Flow records processed: 0, per second: 0, peak per second: 0

Allocation:  
Blocks allocated: 0, per second: 0, peak per second: 0  
Blocks freed: 0, per second: 0, peak per second: 0  
Blocks unavailable: 0, per second: 0, peak per second: 0

Files:  
Files created: 0, per second: 0, peak per second: 0  
Files exported: 0, per second: 0, peak per second: 0  
Files destroyed: 0, per second: 0, peak per second: 0

Throughput:  
Uncompressed bytes: 0, per second: 0, peak per second: 0  
Compressed bytes: 0, per second: 0, peak per second: 0

Packet drops:  
No memory: 0, Not IP: 0  
Not IPv4: 0, Too small: 0  
Fragments: 0, ICMP: 0  
TCP: 0, Unknown: 0  
Not JUNOS flow: 0

File Transfer:  
FTP bytes: 70, per second: 0, peak per second: 6  
FTP files: 0, per second: 0, peak per second: 0  
FTP failure: 0

Export channel: 0  
Current server: Primary  
Primary server state: Unknown, Secondary server state: OK

Export channel: 1



Current server: Primary  
 Primary server state: Unknown, Secondary server state: OK

#### show services flow-collector interface all terse

```
user@host> show services flow-collector interface all terse
Flow collector interface: cp-6/1/0
Interface state: Collecting flows
 Packets Bytes Flows Uncompressed Compressed FTP bytes FTP files
 Bytes Bytes
 4384 6659616 131070 13742307 3786177 3786247 1

Flow collector interface: cp-6/3/0
Interface state: Collecting flows
 Packets Bytes Flows Uncompressed Compressed FTP bytes FTP files
 Bytes Bytes
 0 0 0 0 0 70 0
```

#### show services flow-collector interface extensive

```
user@host> show services flow-collector interface cp-5/2/0 extensive
Flow collector interface: cp-5/2/0
Interface state: Collecting flows
Memory:
 Used: 458311860, Free: 40810008
Input:
 Packets: 922629, per second: 2069, peak per second: 3266
 Bytes: 1376559252, per second: 3096940, peak per second: 4880051
 Flow records processed: 25764957, per second: 42564, peak per second: 98124
Allocation:
 Blocks allocated: 20862, per second: 31, peak per second: 72
 Blocks freed: 17161, per second: 40, peak per second: 202
 Blocks unavailable: 58786, per second: 652, peak per second: 1120
Files:
 Files created: 52, per second: 0, peak per second: 0
 Files exported: 42, per second: 0, peak per second: 0
 Files destroyed: 42, per second: 0, peak per second: 0
Throughput:
 Uncompressed bytes: 2592070401, per second: 7297307,
 peak per second: 8630023
 Compressed bytes: 659600068, per second: 1858458, peak per second: 2198471
Packet drops:
 No memory: 58786, Not IP: 0
 Not IPv4: 0, Too small: 0
 Fragments: 0, ICMP: 0
 TCP: 0, Unknown: 0
 Not JUNOS flow: 0
File Transfer:
 FTP bytes: 585981447, per second: 1313320, peak per second: 4857798
 FTP files: 48, per second: 0, peak per second: 0
 FTP failure: 8
Export channel: 0
 Current server: Primary
 Primary server state: FTP error, Secondary server state: Not configured
Export channel: 1
 Current server: Primary
 Primary server state: OK, Secondary server state: Not configured
```

## show services rpm active-servers

|                                 |                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services rpm active-servers                                                                                                                                                                              |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers. |
| <b>Description</b>              | Display the protocols and corresponding ports for which a router or switch is configured as a real-time performance monitoring (RPM) server.                                                                  |
| <b>Options</b>                  | This command has no options.                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">show services rpm active-servers on page 624</a>                                                                                                                                                  |
| <b>Output Fields</b>            | <a href="#">Table 60 on page 624</a> lists the output fields for the <b>show services rpm active-servers</b> command. Output fields are listed in the approximate order in which they appear.                 |

**Table 60: show services rpm active-servers Output Fields**

| Field Name                        | Field Description                                                                                                                                   |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Protocol</b>                   | Protocol configured on the receiving probe server. The protocol can be the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP). |
| <b>Port</b>                       | Port configured on the receiving probe server.                                                                                                      |
| <b>Destination interface name</b> | Output interface name for the probes.                                                                                                               |

## Sample Output

### show services rpm active-servers

```
user@host> show services rpm active-servers
 Protocol: TCP, Port: 50000, Destination interface name: lt-0/0/0.0
 Protocol: UDP, Port: 50001, Destination interface name: lt-0/0/0.0
```

## show services rpm history-results

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services rpm history-results<br><brief   detail><br><owner <i>owner</i> ><br><since <i>time</i> ><br><test <i>name</i> >                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Display standard information about the results of the last 50 probes for each real-time performance monitoring (RPM) instance.                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>none</b>—Display the results of the last 50 probes for all RPM instances.</p> <p><b>brief   detail</b>—(Optional) Display the specified level of output.</p> <p><b>owner <i>owner</i></b>—(Optional) Display information for the specified probe owner.</p> <p><b>since <i>time</i></b>—(Optional) Display information from the specified time. Specify time as <i>yyyy-mm-dd.hh:mm:ss</i>.</p> <p><b>test <i>name</i></b>—(Optional) Display information for the specified test.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show services rpm history-results on page 626</a><br><a href="#">show services rpm history-results detail on page 626</a>                                                                                                                                                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | Table 61 on page 625 lists the output fields for the <b>show services rpm history-results</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                              |

Table 61: show services rpm history-results Output Fields

| Field Name             | Field Description                                                                                                                                                                                                                                                                                                   | Level of Output |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Owner</b>           | Probe owner.                                                                                                                                                                                                                                                                                                        | All levels      |
| <b>Test</b>            | Name of a test for a probe instance.                                                                                                                                                                                                                                                                                | All levels      |
| <b>Probe received</b>  | Timestamp when the probe result was determined.                                                                                                                                                                                                                                                                     | All levels      |
| <b>Round trip time</b> | Average ping round-trip time (RTT), in microseconds.                                                                                                                                                                                                                                                                | All levels      |
| <b>Probe results</b>   | Result of a particular probe performed by a remote host. The following information is contained in the results: <ul style="list-style-type: none"> <li><b>Response received</b>—Timestamp when the probe result was determined.</li> <li><b>Rtt</b>—Average ping round-trip time (RTT), in microseconds.</li> </ul> | <b>detail</b>   |

Table 61: show services rpm history-results Output Fields (*continued*)

| Field Name                       | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Level of Output |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Results over current test</b> | Displays the results for the current test by probe at the time each probe was completed, as well as the status of the current test at the time the probe was completed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>detail</b>   |
| <b>Probes sent</b>               | Number of probes sent with the current test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>detail</b>   |
| <b>Probes received</b>           | Number of probe responses received within the current test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>detail</b>   |
| <b>Loss percentage</b>           | Percentage of lost probes for the current test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>detail</b>   |
| <b>Measurement</b>               | <p>Increment of measurement. Possible values are round-trip time delay and, for the probe type icmp-pin-timestamp, the egress and ingress delay:</p> <ul style="list-style-type: none"> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Jitter</b>—Difference, in microseconds, between the maximum and minimum RTT measured over the course of the current test.</li> <li>• <b>Stddev</b>—Standard deviation of the round-trip time, in microseconds, measured over the course of the current test.</li> </ul> | <b>detail</b>   |

## Sample Output

### show services rpm history-results

```

user@host> show services rpm history-results
 Owner, Test Probe received Round trip time
p1, t1 Wed Aug 12 01:02:35 2009 315 usec
p1, t1 Wed Aug 12 01:02:36 2009 266 usec
p1, t1 Wed Aug 12 01:02:37 2009 314 usec
p1, t1 Wed Aug 12 01:02:38 2009 388 usec
p1, t1 Wed Aug 12 01:02:39 2009 316 usec
p1, t1 Wed Aug 12 01:02:40 2009 271 usec
p1, t1 Wed Aug 12 01:02:41 2009 314 usec
p1, t1 Wed Aug 12 01:02:42 2009 1180 usec

```

### show services rpm history-results detail

```

user@host> show services rpm history-results detail
Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
 Response received, Wed Aug 12 01:02:35 2009,
 Client and server hardware timestamps
 Rtt: 315 usec
Results over current test:
 Probes sent: 1, Probes received: 1, Loss percentage: 0
Measurement: Round trip time
 Samples: 1, Minimum: 315 usec, Maximum: 315 usec, Average: 315 usec,
 Peak to peak: 0 usec, Stddev: 0 usec, Sum: 315 usec

```

```
Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
 Response received, Wed Aug 12 01:02:36 2009,
 Client and server hardware timestamps
 Rtt: 266 usec, Round trip jitter: -50 usec,
 Round trip interarrival jitter: 3 usec
Results over current test:
 Probes sent: 2, Probes received: 2, Loss percentage: 0
 Measurement: Round trip time
 Samples: 2, Minimum: 266 usec, Maximum: 315 usec, Average: 291 usec,
 Peak to peak: 49 usec, Stddev: 24 usec, Sum: 581 usec
 Measurement: Negative round trip jitter
 Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
 Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
 Response received, Wed Aug 12 01:02:37 2009,
 Client and server hardware timestamps
 Rtt: 314 usec, Round trip jitter: 49 usec,
 Round trip interarrival jitter: 6 usec
Results over current test:
 Probes sent: 3, Probes received: 3, Loss percentage: 0
 Measurement: Round trip time
 Samples: 3, Minimum: 266 usec, Maximum: 315 usec, Average: 298 usec,
 Peak to peak: 49 usec, Stddev: 23 usec, Sum: 895 usec
 Measurement: Positive round trip jitter
 Samples: 1, Minimum: 49 usec, Maximum: 49 usec, Average: 49 usec,
 Peak to peak: 0 usec, Stddev: 0 usec, Sum: 49 usec
 Measurement: Negative round trip jitter
 Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
 Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
 Response received, Wed Aug 12 01:02:38 2009,
 Client and server hardware timestamps
 Rtt: 388 usec, Round trip jitter: 74 usec,
 Round trip interarrival jitter: 10 usec
Results over current test:
 Probes sent: 4, Probes received: 4, Loss percentage: 0
 Measurement: Round trip time
 Samples: 4, Minimum: 266 usec, Maximum: 388 usec, Average: 321 usec,
 Peak to peak: 122 usec, Stddev: 44 usec, Sum: 1283 usec
 Measurement: Positive round trip jitter
 Samples: 2, Minimum: 49 usec, Maximum: 74 usec, Average: 62 usec,
 Peak to peak: 25 usec, Stddev: 12 usec, Sum: 123 usec
 Measurement: Negative round trip jitter
 Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
 Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec
```

## show services rpm probe-results

|                                 |                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show services rpm probe-results</code><br><code>&lt;owner owner&gt;</code><br><code>&lt;test name&gt;</code>                                                                                                                               |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 13.2 for PTX Series Packet Transport Series Routers.                             |
| <b>Description</b>              | Display the results of the most recent real-time performance monitoring (RPM) probes.                                                                                                                                                            |
| <b>Options</b>                  | <b>none</b> —Display all results of the most recent RPM probes.<br><br><b>owner owner</b> —(Optional) Display information for the specified probe owner.<br><br><b>test name</b> —(Optional) Display information for the specified test.         |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                             |
| <b>List of Sample Output</b>    | <a href="#">show services rpm probe-results (IPv4 Targets) on page 631</a><br><a href="#">show services rpm probe-results (IPv6 Targets) on page 633</a><br><a href="#">show services rpm probe-results (BGP Neighbor Discovery) on page 634</a> |
| <b>Output Fields</b>            | <a href="#">Table 62 on page 628</a> lists the output fields for the <b>show services rpm probe-results</b> command. Output fields are listed in the approximate order in which they appear.                                                     |

**Table 62: show services rpm probe-results Output Fields**

| Field Name                  | Field Description                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Owner</b>                | Owner name. When you configure the probe owner statement at the <b>[edit services rpm]</b> hierarchy level, this field displays the configured owner name. When you configure BGP neighbor discovery through RPM, the output for this field is <b>Rpm-Bgp-Owner</b> .                                                                                              |
| <b>Test</b>                 | Name of a test representing a collection of probes. When you configure the test test-name statement at the <b>[edit services rpm probe owner]</b> hierarchy level, the field displays the configured test name. When you configure BGP neighbor discovery through RPM, the output for this field is <b>Rpm-BGP-Test-n</b> , where <i>n</i> is a cumulative number. |
| <b>Target address</b>       | Destination IPv4 address used for the probes. This field is displayed when the probes are sent to the configured IPv4 targets or RPM servers.                                                                                                                                                                                                                      |
| <b>Target inet6-address</b> | Destination IPv6 address used for the probes. This field is displayed when the probes are sent to the configured IPv6 targets or RPM servers.                                                                                                                                                                                                                      |
| <b>Source address</b>       | Source address used for the probes.                                                                                                                                                                                                                                                                                                                                |
| <b>Probe type</b>           | Protocol configured on the receiving probe server: <b>http-get</b> , <b>http-metadata-get</b> , <b>icmp-ping</b> , <b>icmp-ping-timestamp</b> , <b>tcp-ping</b> , <b>udp-ping</b> , or <b>udp-ping-timestamp</b> .                                                                                                                                                 |

Table 62: show services rpm probe-results Output Fields (*continued*)

| Field Name                   | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Test size</b>             | Number of probes within a test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Routing Instance Name</b> | <p>(BGP neighbor discovery) Name of the configured (if any) routing instance, logical system name, or both, in which the probe is configured:</p> <ul style="list-style-type: none"> <li>When a routing instance is defined within a logical system, the logical system name is followed by the routing instance name. A slash ( / ) is used to separate the two entities. For example, if the routing instance called <b>R1</b> is configured within the logical system called <b>LS</b>, the name in the output field is <b>LS/R1</b>.</li> <li>When a routing instance is configured but the default logical system is used, the name in the output field is the name of the routing instance.</li> <li>When a logical system is configured but the default routing instance is used, the name in the output field is the name of the logical system followed by <b>default</b>. A slash ( / ) is used to separate the two entities. For example, <b>LS/default</b>.</li> </ul>                                    |
| <b>Probe results</b>         | <p>Raw measurement of a particular probe sample done by a remote host. This data is provided separately from the calculated results. The following information is contained in the raw measurement:</p> <ul style="list-style-type: none"> <li><b>Response received</b>—Timestamp when the probe result was determined.</li> <li><b>Client and server hardware timestamps</b>—If timestamps are configured, an entry appears at this point.</li> <li><b>Rtt</b>—Average ping round-trip time (RTT), in microseconds.</li> <li><b>Egress jitter</b>—Egress jitter, in microseconds.</li> <li><b>Ingress jitter</b>—Ingress jitter, in microseconds.</li> <li><b>Round trip jitter</b>—Round-trip jitter, in microseconds.</li> <li><b>Egress interarrival jitter</b>—Egress interarrival jitter, in microseconds.</li> <li><b>Ingress interarrival jitter</b>—Ingress interarrival jitter, in microseconds.</li> <li><b>Round trip interarrival jitter</b>—Round-trip interarrival jitter, in microseconds.</li> </ul> |

Table 62: show services rpm probe-results Output Fields (*continued*)

| Field Name                       | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Results over current test</b> | <p>Probes are grouped into tests, and the statistics are calculated for each test. If a test contains 10 probes, the average, minimum, and maximum results are calculated from the results of those 10 probes. If the command is issued while the test is in progress, the statistics use information from the completed probes.</p> <ul style="list-style-type: none"> <li>• <b>Probes sent</b>—Number of probes sent within the current test.</li> <li>• <b>Probes received</b>—Number of probe responses received within the current test.</li> <li>• <b>Loss percentage</b>—Percentage of lost probes for the current test.</li> <li>• <b>Measurement</b>—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type <b>icmp-ping-timestamp</b>, the egress delay and ingress delay.</li> </ul> <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> <li>• <b>Samples</b>—Number of probes.</li> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Peak to peak</b>—Peak-to-peak difference, in microseconds.</li> <li>• <b>Stddev</b>—Standard deviation, in microseconds.</li> <li>• <b>Sum</b>—Statistical sum.</li> </ul> |
| <b>Results over last test</b>    | <p>Results for the most recently completed test. If the command is issued while the first test is in progress, this information is not displayed</p> <ul style="list-style-type: none"> <li>• <b>Probes sent</b>—Number of probes sent for the most recently completed test.</li> <li>• <b>Probes received</b>—Number of probe responses received for the most recently completed test.</li> <li>• <b>Loss percentage</b>—Percentage of lost probes for the most recently completed test.</li> <li>• <b>Test completed</b>—Time the most recent test was completed.</li> <li>• <b>Measurement</b>—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type <b>icmp-ping-timestamp</b>, the egress delay and ingress delay.</li> </ul> <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> <li>• <b>Samples</b>—Number of probes.</li> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured for the most recently completed test.</li> <li>• <b>Peak to peak</b>—Peak-to-peak difference, in microseconds.</li> <li>• <b>Stddev</b>—Standard deviation, in microseconds.</li> <li>• <b>Sum</b>—Statistical sum.</li> </ul>                                                          |



Table 62: show services rpm probe-results Output Fields (*continued*)

| Field Name                    | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Results over all tests</b> | <p>Displays statistics made for all the probes, independently of the grouping into tests, as well as statistics for the current test.</p> <ul style="list-style-type: none"> <li>• <b>Probes sent</b>—Number of probes sent in all tests.</li> <li>• <b>Probes received</b>—Number of probe responses received in all tests.</li> <li>• <b>Loss percentage</b>—Percentage of lost probes in all tests.</li> <li>• <b>Measurement</b>—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe types <b>icmp-ping-timestamp</b> and <b>udp-ping-timestamp</b>, the egress delay and ingress delay.</li> </ul> <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> <li>• <b>Samples</b>—Number of probes.</li> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Peak to peak</b>—Peak-to-peak difference, in microseconds.</li> <li>• <b>Stddev</b>—Standard deviation, in microseconds.</li> <li>• <b>Sum</b>—Statistical sum.</li> </ul> |
| <b>Error Stats</b>            | <p>Displays error statistics for each probe.</p> <ul style="list-style-type: none"> <li>• <b>Invalid client rcv timestamp</b>—Number of client receive timestamp less than client send timestamp.</li> <li>• <b>Invalid server send timestamp</b>—Number of server send timestamp less than server receive timestamp.</li> <li>• <b>Invalid server processing time</b>—Number of server side spent time greater than RTT.</li> </ul> <p><b>NOTE:</b> <b>Error Stats</b> is displayed in the output only if non-zero statistics exists.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Sample Output

### show services rpm probe-results (IPv4 Targets)

```

user@host> show services rpm probe-results
Owner: ADSN-J4300.ADSN-J2300.D2, Test: 75300002
Target address: 172.16.54.172, Source address: 10.206.0.1,
Probe type: udp-ping-timestamp, Test size: 10 probes
Probe results:
 Response received, Tue Feb 6 14:53:15 2007,
 Client and server hardware timestamps
 Rtt: 575 usec, Egress jitter: 5 usec, Ingress jitter: 8 usec,
 Round trip jitter: 12 usec, Egress interarrival jitter: 8 usec,
 Ingress interarrival jitter: 7 usec, Round trip interarrival jitter: 7 usec,

 Round trip interarrival jitter: 669 usec
Results over current test:
 Probes sent: 10, Probes received: 10, Loss percentage: 0
 Measurement: Round trip time
 Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
 Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec

```

Measurement: Positive round trip jitter  
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,  
Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec  
Measurement: Negative round trip jitter  
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,  
Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec  
Measurement: Egress time  
Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,  
Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec  
Measurement: Positive Egress jitter  
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,  
Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec  
Measurement: Negative Egress jitter  
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,  
Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec  
Measurement: Ingress time  
Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,  
Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec  
Measurement: Positive Ingress jitter  
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,  
Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec  
Measurement: Negative Ingress jitter  
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,  
Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec  
Results over last test:  
Probes sent: 10, Probes received: 10, Loss percentage: 0  
Test completed on Tue Feb 6 14:53:16 2007  
Measurement: Round trip time  
Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,  
Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec  
Measurement: Positive round trip jitter  
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,  
Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec  
Measurement: Negative round trip jitter  
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,  
Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec  
Measurement: Egress time  
Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,  
Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec  
Measurement: Positive Egress jitter  
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,  
Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec  
Measurement: Negative Egress jitter  
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,  
Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec  
Measurement: Ingress time  
Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,  
Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec  
Measurement: Positive Ingress jitter  
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,  
Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec  
Measurement: Negative Ingress jitter  
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,  
Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec  
Results over all tests:  
Probes sent: 560, Probes received: 560, Loss percentage: 0  
Measurement: Round trip time  
Samples: 560, Minimum: 805 usec, Maximum: 3114 usec, Average: 1756 usec,  
Peak to peak: 2309 usec, Stddev: 519 usec, Sum: xxxx usec  
Measurement: Positive round trip jitter

```

 Samples: 257, Minimum: 0 usec, Maximum: 2054 usec, Average: 597 usec,
 Peak to peak: 2054 usec, Stddev: 427 usec, Sum: xxxx usec
Measurement: Negative round trip jitter
 Samples: 302, Minimum: 1 usec, Maximum: 1812 usec, Average: 511 usec,
 Peak to peak: 1811 usec, Stddev: 408 usec, Sum: xxxx usec
Measurement: Egress time
 Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
 Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
Measurement: Positive Egress jitter
 Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
 Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
Measurement: Negative Egress jitter
 Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
 Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Measurement: Ingress time
 Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
 Peak to peak: 2054 usec, Stddev: 738 usec, Sum: xxxx usec
Measurement: Positive Ingress jitter
 Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
 Peak to peak: 2049 usec, Stddev: 679 usec, Sum: xxxx usec
Measurement: Negative Ingress jitter
 Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
 Peak to peak: 1807 usec, Stddev: 665 usec, Sum: xxxx usec
Error Stats:
 Invalid client recv timestamp: 3, Invalid server send timestamp: 0
 Invalid server processing time: 0

```

#### show services rpm probe-results (IPv6 Targets)

```

user@host> show services rpm probe-results
Owner: p, Test: t1
Target inet6-address: 2001:db8:0:1:2a0:a502:0:1da,
Target Port : 34567 Test size: 1000000 probes
Probe results:
 Response received, Mon Dec 16 10:48:07 2013, Client and server hardware
timestamps
 Rtt: 236 usec, Round trip jitter: -10 usec, Round trip interarrival jitter:
484 usec
 Results over current test:
 Probes sent: 10, Probes received: 10, Loss percentage: 0
 Measurement: Round trip time
 Samples: 10, Minimum: 231 usec, Maximum: 298 usec, Average: 268 usec,
Peak to peak: 67 usec, Stddev: 24 usec, Sum: 2682 usec
 Measurement: Positive round trip jitter
 Samples: 3, Minimum: 15 usec, Maximum: 1841 usec, Average: 750 usec, Peak
to peak: 1826 usec, Stddev: 787 usec, Sum: 2251 usec
 Measurement: Negative round trip jitter
 Samples: 7, Minimum: 10 usec, Maximum: 1244 usec, Average: 709 usec, Peak
to peak: 1234 usec, Stddev: 466 usec, Sum: 4961 usec
 Results over last test:
 Probes sent: 10, Probes received: 10, Loss percentage: 0
 Test completed on Mon Dec 16 10:48:07 2013
 Measurement: Round trip time
 Samples: 10, Minimum: 231 usec, Maximum: 298 usec, Average: 268 usec,
Peak to peak: 67 usec, Stddev: 24 usec, Sum: 2682 usec
 Measurement: Positive round trip jitter
 Samples: 3, Minimum: 15 usec, Maximum: 1841 usec, Average: 750 usec, Peak
to peak: 1826 usec, Stddev: 787 usec, Sum: 2251 usec
 Measurement: Negative round trip jitter
 Samples: 7, Minimum: 10 usec, Maximum: 1244 usec, Average: 709 usec, Peak
to peak: 1234 usec, Stddev: 466 usec, Sum: 4961 usec

```

```
Results over all tests(From start of current control session):
 Probes sent: 490, Probes received: 488, Loss percentage: 0
 Measurement: Round trip time
 Samples: 488, Minimum: 231 usec, Maximum: 306 usec, Average: 270 usec,
Peak to peak: 75 usec, Stddev: 16 usec, Sum: 131586 usec
 Measurement: Positive round trip jitter
 Samples: 254, Minimum: 0 usec, Maximum: 10151 usec, Average: 157 usec,
Peak to peak: 10151 usec, Stddev: 873 usec, Sum: 39817 usec
 Measurement: Negative round trip jitter
 Samples: 233, Minimum: 1 usec, Maximum: 10170 usec, Average: 171 usec,
Peak to peak: 10169 usec, Stddev: 888 usec, Sum: 39889 usec
```

#### **show services rpm probe-results (BGP Neighbor Discovery)**

```
user@host> show services rpm probe-results
Owner: Rpm-Bgp-Owner, Test: Rpm-Bgp-Test-1
Target address: 10.209.152.37, Probe type: icmp-ping, Test size: 5 probes
Routing Instance Name: LS1/RI1
Probe results:
 Response received, Fri Oct 28 05:20:23 2005
 Rtt: 662 usec
Results over current test:
 Probes sent: 5, Probes received: 5, Loss percentage: 0
 Measurement: Round trip time
 Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
 Jitter: 133 usec, Stddev: 53 usec
Results over all tests:
 Probes sent: 5, Probes received: 5, Loss percentage: 0
 Measurement: Round trip time
 Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
 Jitter: 133 usec, Stddev: 53 usec
```

## show services rpm rfc2544-benchmarking

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show services rpm rfc2544-benchmarking &lt;aborted-tests (test-id test-id   brief   detail)&gt; &lt;active-tests (test-id test-id   brief   detail)&gt; &lt;completed-tests (test-id test-id   brief   detail)&gt; &lt;summary&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | <p>Command introduced in Junos OS Release 12.3X52 for ACX Series routers.</p> <p>Command introduced in Junos OS Release 13.3R1 for MX104 3D Universal Edge Routers.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <p>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. You can view the results of each test state for all of the configured test IDs or for a specific test ID. Also, you can display statistics about the total number of tests of each state for a high-level, quick analysis. The values in the output displayed vary, depending on the state in which the test is passing through, when you issue the command.</p> <p>You can view the test results of multiple test IDs at the same time by entering the IDs in a single command. If you enter multiple test ID values, you must separate each number with a space.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                  | <p><b>aborted-tests</b>—Display the list of tests that were aborted or stopped. This list includes tests that failed due to various error conditions and tests that you terminated by entering the <b>test service rpm rfc2544-benchmarking test test-name stop</b> command. The <b>Status</b> field in the output specifies the reason for the termination of the test.</p> <p><b>test-id test-id</b>—Unique identifier of the test for which the test results must be displayed.</p> <p><b>brief   detail</b>—(Optional) Display the specified level of output.</p> <p><b>active-tests</b>—Display the results of the set of tests that are currently running.</p> <p><b>completed-tests</b>—Display the results of the set of tests that were successfully completed. A completed test is one that passes through all the test steps or states specified in RFC 2544. A test that is marked as completed after it went through all the states from the beginning to the end can still be reported as a failed test. For example, a failed test can be a test that sends the desired number of packets, but does not receive the frames back from the other end.</p> <p><b>summary</b>—(Optional) Display summary output.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li> <li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li> <li>• <a href="#">rfc2544-benchmarking on page 477</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**List of Sample Output** [show services rpm rfc2544-benchmarking summary on page 637](#)  
[show services rpm rfc2544-benchmarking aborted-tests \(ACX Series router\) on page 637](#)  
[show services rpm rfc2544-benchmarking completed-tests \(ACX Series router\) on page 637](#)  
[show services rpm rfc2544-benchmarking active-tests \(ACX Series router\) on page 638](#)  
[show services rpm rfc2544-benchmarking aborted-tests \(MX104 router\) on page 638](#)  
[show services rpm rfc2544-benchmarking completed-tests \(MX104 router\) on page 638](#)  
[show services rpm rfc2544-benchmarking active-tests \(MX104 router\) on page 639](#)

**Output Fields** [Table 63 on page 636](#) lists the output fields for the **show services rpm rfc2544-benchmarking** command. Output fields are listed in the approximate order in which they appear.

**Table 63: show services rpm rfc2544-benchmarking Output Fields**

| Field Name                   | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Test information</b>      | Details of the performed RFC 2544 benchmarking test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Test id</b>               | Unique identifier configured for the test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Test name</b>             | Name configured for the test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Test type</b>             | The type of statistical detail that is collected for the test, based on the configured test type. Throughput-related, latency, frame-loss, or back-to-back frames-related information is displayed for ACX Series routers. Reflected packets-related information is displayed for MX104 routers..                                                                                                                                                                                                                                  |
| <b>Test mode</b>             | Mode configured for the test on the router. Test modes are: <ul style="list-style-type: none"> <li>Initiate-and-Terminate: Test frames are initiated from one end and terminated at the same end. This mode requires a reflector to be configured at the peer end to enable the test frames to be returned to the source. This mode is supported only on ACX Series routers</li> <li>Reflect: Test frames that originate from one end are reflected at the other end on the selected service, such as IPv4 or Ethernet.</li> </ul> |
| <b>Test packet size</b>      | Size of the test packets in bytes. This field is valid only when the test mode is Initiate-and-Terminate.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Test state</b>            | State of the test that is in progress or active when the output is displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Status</b>                | Indicates whether the test is currently in progress or has been terminated. This field is displayed for tests that are in progress or were aborted by entering the <b>test services rpm rfc2544-benchmarking test &lt;test-name   test-id&gt; stop</b> command.                                                                                                                                                                                                                                                                    |
| <b>Test start time</b>       | Time at which the test started in Coordinated Universal Time (UTC) format (YYYY-MM-DD-HH:MM:SS).                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Test finish time</b>      | Time at which the test completed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Counters last cleared</b> | Date, time, and how long ago the statistics for the test were cleared. The format is <i>year-month-day hour:minute:second:timezone</i> ( <i>hour:minute:second</i> ago). For example, 2010-05-17 07:51:28 PDT (00:04:33 ago). If you did not clear the statistics previously at any point, <b>Never</b> is displayed.                                                                                                                                                                                                              |

Table 63: show services rpm rfc2544-benchmarking Output Fields (*continued*)

| Field Name                | Field Description                                      |
|---------------------------|--------------------------------------------------------|
| Number of active tests    | Total number of tests that are currently running.      |
| Number of completed tests | Total number of tests that were successfully completed |
| Number of aborted tests   | Total number of tests that were aborted or halted.     |

## Sample Output

### show services rpm rfc2544-benchmarking summary

```
user@host> show services rpm rfc2544-benchmarking summary
```

Rfc2544 tests summary :

Number of active tests: 0, Number of completed tests: 4, Number of aborted tests: 52

This output indicates that no test iteration is currently in progress (at the time of issue of the command), 4 tests were completed successfully, and 52 tests were halted.

### show services rpm rfc2544-benchmarking aborted-tests (ACX Series router)

```
user@host> show services rpm rfc2544-benchmarking aborted-tests
```

Test information :

```
Test id: 1, Test name: test1, Test type: Throughput
Test mode: Initiate-and-Terminate
Test packet size: 64 1280
Test state: RFC2544_TEST_STATE_STOPPED
Status: User-aborted-via-cli
Test start time: 2005-08-05 03:19:58 UTC
Test finish time: 2005-08-05 03:20:00 UTC
Counters last cleared: Never
```

```
Test id: 2, Test name: test1, Test type: Throughput
Test mode: Initiate-and-Terminate
Test packet size: 64 1280
Test state: RFC2544_TEST_STATE_STOPPED
Status: User-aborted-via-cli
Test start time: 2005-08-05 03:20:00 UTC
Test finish time: 2005-08-05 03:20:02 UTC
Counters last cleared: Never
```

### show services rpm rfc2544-benchmarking completed-tests (ACX Series router)

```
user@host> show services rpm rfc2544-benchmarking completed-tests
```

Test information :

```
Test id: 18, Test name: test1, Test type: Throughput
Test mode: Initiate-and-Terminate
Test packet size: 64 1280
Test state: RFC2544_TEST_STATE_COMPLETED
Test start time: 2005-08-05 03:20:34 UTC
```

Test finish time: 2005-08-05 03:21:23 UTC  
Counters last cleared: Never

#### show services rpm rfc2544-benchmarking active-tests (ACX Series router)

```
user@host> show services rpm rfc2544-benchmarking active-tests
Test information :
 Test id: 57, Test name: test1, Test type: Back-Back-Frames
 Test mode: Initiate-and-Terminate
 Test packet size: 64 1280
 Test state: RFC2544_TEST_STATE_RUNNING
 Status: Running
 Test start time: 2005-08-05 20:15:41 UTC
 Test finish time: TEST_RUNNING
 Counters last cleared: Never
```

#### show services rpm rfc2544-benchmarking aborted-tests (MX104 router)

```
user@host> show services rpm rfc2544-benchmarking aborted-tests
Test information :
 Test id: 1, Test name: prof_tput1, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: TEST_STATE_STOPPED
 Status: Test-intf-ifl-change
 Test start time: 2013-12-16 22:54:27 PST
 Test finish time: 2013-12-16 23:30:28 PST
 Counters last cleared: Never

 Test id: 2, Test name: prof_tput1, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: TEST_STATE_STOPPED
 Status: User-aborted-via-cli
 Test start time: 2013-12-16 23:31:06 PST
 Test finish time: 2013-12-16 23:36:22 PST
 Counters last cleared: Never

 Test id: 3, Test name: prof_tput1, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: TEST_STATE_STOPPED
 Status: User-aborted-via-cli
 Test start time: 2013-12-16 23:36:24 PST
 Test finish time: 2013-12-17 01:49:24 PST
 Counters last cleared: Never
```

#### show services rpm rfc2544-benchmarking completed-tests (MX104 router)

```
user@host> show services rpm rfc2544-benchmarking completed-tests
Test information :
 Test id: 18, Test name: test1, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: TEST_STATE_COMPLETED
 Test start time: 2005-08-05 03:20:34 UTC
 Test finish time: 2005-08-05 03:21:23 UTC
 Counters last cleared: Never
```



**show services rpm rfc2544-benchmarking active-tests (MX104 router)**

```
user@host> show services rpm rfc2544-benchmarking active-tests
Test information :
 Test id: 4, Test name: prof_tput1, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: TEST_STATE_RUNNING
 Status: Running
 Test start time: 2013-12-17 01:49:26 PST
 Test finish time: TEST_RUNNING
 Counters last cleared: Never
```

## **show services rpm rfc2544-benchmarking test-id**

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show services rpm rfc2544-benchmarking test-id <i>test-id</i></code><br><code>&lt;brief   detail&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.3X52 for ACX Series routers.<br>Command introduced in Junos OS Release 13.3R1 for MX104 3D Universal Edge Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Display information about the results of the RFC 2544-based benchmarking test for a specific test ID for each real-time performance monitoring (RPM) instance. The values in the output displayed vary, depending on the state in which the test is passing through, when you issue the command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <b>none</b> —Display brief information about a specific test ID of the benchmarking test.<br><br><b>test-id <i>test-id</i></b> —Unique identifier of the test for which the test results must be displayed.<br><br><b>brief   detail</b> —(Optional) Display the specified level of output.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring an RFC 2544-Based Benchmarking Test on page 235</a></li><li>• <a href="#">RFC2544-Based Benchmarking Tests Overview on page 227</a></li><li>• <a href="#">rfc2544-benchmarking on page 477</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>List of Sample Output</b>    | <a href="#">show services rpm rfc2544-benchmarking test-id detail (Throughput Test on ACX Series routers ) on page 648</a><br><a href="#">show services rpm rfc2544-benchmarking test-id detail (Latency Test on ACX Series routers) on page 649</a><br><a href="#">show services rpm rfc2544-benchmarking test-id detail (Frame Loss Test on ACX Series routers) on page 652</a><br><a href="#">show services rpm rfc2544-benchmarking test-id detail (Back-to-Back Frames Test on ACX Series routers) on page 653</a><br><a href="#">show services rpm rfc2544-benchmarking test-id detail (Reflection Test on MX104 routers) on page 654</a><br><a href="#">show services rpm rfc2544-benchmarking test-id brief (Reflection Test on MX104 routers) on page 655</a><br><a href="#">show services rpm rfc2544-benchmarking test-id detail (Reflection Test on MX104 routers) on page 655</a><br><a href="#">show services rpm rfc2544-benchmarking test-id brief (Reflection Test on MX104 routers) on page 656</a> |
| <b>Output Fields</b>            | <a href="#">Table 64 on page 641</a> lists the output fields for the <b>show services rpm rfc2544-benchmarking test-id</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Table 64: show services rpm rfc2544-benchmarking test-id Output Fields

| Field Name                        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Level of Output |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Test information</b>           | Details of the performed RFC 2544 benchmarking test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | None specified  |
| <b>Test id</b>                    | Unique identifier configured for the test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | None specified  |
| <b>Test name</b>                  | Name configured for the test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | None specified  |
| <b>Test type</b>                  | The type of statistical detail that is collected for the test, based on the configured test type. Throughput-related, latency, frame-loss, or back-to-back frames-related information is displayed for ACX Series routers. Reflected packets-related information is displayed for MX104 routers.                                                                                                                                                                                                                                    | None specified  |
| <b>Test mode</b>                  | Mode configured for the test on the router. Test modes are: <ul style="list-style-type: none"> <li>Initiate-and-Terminate: Test frames are initiated from one end and terminated at the same end. This mode requires a reflector to be configured at the peer end to enable the test frames to be returned to the source. This mode is supported only on ACX Series routers.</li> <li>Reflect: Test frames that originate from one end are reflected at the other end on the selected service, such as IPv4 or Ethernet.</li> </ul> | None specified  |
| <b>Test packet size</b>           | Size of the test packets in bytes. This field is valid only when the test mode is Initiate-and-Terminate.                                                                                                                                                                                                                                                                                                                                                                                                                           | None specified  |
| <b>Test state</b>                 | State of the test that is in progress or active when the output is displayed. For details about the states, see <i>RFC 2544-Based Benchmarking Test States</i> .                                                                                                                                                                                                                                                                                                                                                                    | None specified  |
| <b>Status</b>                     | Indicates whether the test is currently in progress or has been terminated.                                                                                                                                                                                                                                                                                                                                                                                                                                                         | None specified  |
| <b>Test start time</b>            | Time at which the test started in Coordinated Universal Time (UTC) format (YYYY-MM-DD-HH:MM:SS).                                                                                                                                                                                                                                                                                                                                                                                                                                    | None specified  |
| <b>Test finish time</b>           | Time at which the test completed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | None specified  |
| <b>Counters last cleared</b>      | Date, time, and how long ago the statistics for the test were cleared. The format is <i>year-month-day hour:minute:second:timezone (hour:minute:second ago)</i> . For example, 2010-05-17 07:51:28 PDT (00:04:33 ago). If you did not clear the statistics previously at any point, <b>Never</b> is displayed.                                                                                                                                                                                                                      | None specified  |
| <b>Test-profile Configuration</b> | (ACX Series routers only) Details of the specified test profile                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <b>detail</b>   |
| <b>Test-profile name</b>          | (ACX Series routers only) Name of the configured test profile that contains the parameters for the test                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>detail</b>   |
| <b>Test packet size</b>           | (ACX Series routers only) Size of the test packets in bytes                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>detail</b>   |
| <b>Theoretical max bandwidth</b>  | (ACX Series routers only) Theoretical maximum bandwidth configured for the test. This value is typically set to the bandwidth of the server being tested. Valid values are 1 Kbps through 1,000,000 Kbps (1 Gbps). The value defined is the highest bandwidth value tested for this test.                                                                                                                                                                                                                                           | <b>detail</b>   |

Table 64: show services rpm rfc2544-benchmarking test-id Output Fields (*continued*)

| Field Name                       | Field Description                                                                                                                                                                                                                                                                  | Level of Output |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Test Configuration</b>        | Details of the configured test ID.                                                                                                                                                                                                                                                 | <b>detail</b>   |
| <b>Test mode</b>                 | Mode configured for the test. Test modes are Initiate-and-Terminate and Reflect.                                                                                                                                                                                                   | <b>detail</b>   |
| <b>Duration in seconds</b>       | Period in seconds for which the test has been performed.                                                                                                                                                                                                                           | <b>detail</b>   |
| <b>Test family</b>               | The underlying service on which the test is run. Test families are: <ul style="list-style-type: none"> <li>INET: Indicates that the test is run on a IPv4 service.</li> <li>CCC: Indicates that the test is run on a circuit cross-connect (CCC) or pseudowire service.</li> </ul> | <b>detail</b>   |
| <b>Routing Instance Name</b>     | (ACX Series routers only) Name of the routing instance for the test                                                                                                                                                                                                                | <b>detail</b>   |
| <b>Inet family Configuration</b> | Details of the configured <b>inet</b> family for an IPv4 service                                                                                                                                                                                                                   | <b>detail</b>   |
| <b>Egress Interface</b>          | Name of the egress interface from which the test frames are sent                                                                                                                                                                                                                   | <b>detail</b>   |
| <b>Source ipv4 address</b>       | Source IPv4 address used in the IP header of the generated test frame.                                                                                                                                                                                                             | <b>detail</b>   |
| <b>Destination ipv4 address</b>  | Destination IPv4 address used in the IP header of the generated test frame.                                                                                                                                                                                                        | <b>detail</b>   |
| <b>Source udp port</b>           | Source UDP port number used in the UDP header of the generated test frame.                                                                                                                                                                                                         | <b>detail</b>   |
| <b>Destination udp port</b>      | Destination UDP port number used in the UDP header of the generated test frame.                                                                                                                                                                                                    | <b>detail</b>   |
| <b>Ccc family Configuration</b>  | Details of the configured CCC family for an Ethernet service                                                                                                                                                                                                                       | <b>detail</b>   |
| <b>Source MAC address</b>        | (ACX Series routers only) Source MAC address used in generated test frames for a CCC or Ethernet pseudowire service.                                                                                                                                                               | <b>detail</b>   |
| <b>Destination MAC address</b>   | (ACX Series routers only) Destination MAC address used in generated test frames for a CCC or Ethernet pseudowire service.                                                                                                                                                          | <b>detail</b>   |
| <b>Ivlan-id</b>                  | (ACX Series routers only) Inner VLAN ID for test-frames.                                                                                                                                                                                                                           | <b>detail</b>   |
| <b>Ovlan-id</b>                  | (ACX Series routers only) Outer VLAN ID for test-frames.                                                                                                                                                                                                                           | <b>detail</b>   |
| <b>Direction egress</b>          | Test is run in the egress direction of the interface (NNI)                                                                                                                                                                                                                         | <b>detail</b>   |
| <b>Direction ingress</b>         | Test is run in the ingress direction of the interface (UNI)                                                                                                                                                                                                                        | <b>detail</b>   |

Table 64: show services rpm rfc2544-benchmarking test-id Output Fields (*continued*)

| Field Name                                  | Field Description                                                                                                                                                          | Level of Output |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Rfc2544 throughput test information         | (ACX Series routers only) Details of the throughput test                                                                                                                   | detail          |
| Initial test load percentage                | Percentage of the steady state load for the test.                                                                                                                          | detail          |
| Test iteration mode                         | Mode of the test iteration: Binary or step-down.                                                                                                                           | detail          |
| Test iteration step percent                 | The test step percentage for tests. If not specified, the default step-percent is 10 percent. This parameter is ignored for all type of tests other than frame-loss tests. | detail          |
| Theoretical max bandwidth                   | The theoretical limit of the media for the frame size configured for the test. This value is typically set to the bandwidth of the server being tested.                    | detail          |
| Test packet size:                           | Packet size of the test frames in bytes.                                                                                                                                   | detail          |
| Iteration                                   | Number of the test iteration.                                                                                                                                              | detail          |
| Duration (sec)                              | Period in seconds for which the test iteration is run                                                                                                                      | detail          |
| Elapsed time                                | Amount of time that has passed, in seconds, since the start of the test.                                                                                                   | detail          |
| pps                                         | Total count of packets-per-second (pps) transmitted during the test.                                                                                                       | detail          |
| Tx Packets                                  | Number of transmitted test packets.                                                                                                                                        | detail          |
| Rx Packets                                  | Number of received test packets.                                                                                                                                           | detail          |
| Tx Bytes                                    | Number of transmitted bytes.                                                                                                                                               | detail          |
| Rx Bytes                                    | Number of received bytes.                                                                                                                                                  | detail          |
| Percentage throughput                       | Percentage of throughput for the test iteration.                                                                                                                           | detail          |
| Result of the iteration runs (Throughput) : | Results of the completed throughput test for a particular packet size.                                                                                                     | detail          |
| Best iteration                              | Number of the iteration with the highest throughout, among the listed iterations.                                                                                          | detail          |
| Best iteration (pps)                        | Packets-per-second (pps) count of the iteration with the highest throughout, among the listed iterations.                                                                  | detail          |
| Best iteration throughput                   | Percentage of throughput of the iteration with the highest throughout, among the listed iterations.                                                                        | detail          |

Table 64: show services rpm rfc2544-benchmarking test-id Output Fields (*continued*)

| Field Name                                     | Field Description                                                                                                                                                                                                                                             | Level of Output       |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>RFC2544 Throughput test results summary</b> | Consolidated information of the throughput test.                                                                                                                                                                                                              | <b>detail summary</b> |
| <b>Packet Size</b>                             | Size of the test packet in bytes.                                                                                                                                                                                                                             | <b>detail summary</b> |
| <b>Theoretical rate (pps)</b>                  | Theoretical frame rate in packets-per-second.                                                                                                                                                                                                                 | <b>detail summary</b> |
| <b>Tx Packets</b>                              | Number of transmitted packets.                                                                                                                                                                                                                                | <b>detail summary</b> |
| <b>Rx Packets</b>                              | Number of received packets.                                                                                                                                                                                                                                   | <b>detail summary</b> |
| <b>Offered throughput (percentage)</b>         | The offered throughput in percentage of the chosen service (such as Layer 3 or Ethernet pseudowire).                                                                                                                                                          | <b>detail summary</b> |
| <b>Measured bandwidth (kbps)</b>               | Available bandwidth of the service based on the calculated throughput.                                                                                                                                                                                        | <b>detail summary</b> |
| <b>Rfc2544 latency test information :</b>      | <b>(ACX Series routers only) Details of the latency test</b>                                                                                                                                                                                                  | <b>detail</b>         |
| <b>Theoretical max bandwidth</b>               | Theoretical maximum bandwidth configured for the test. This value is typically set to the bandwidth of the server being tested. Valid values are 1 Kbps through 1,000,000 Kbps (1 Gbps). The value defined is the highest bandwidth value used for this test. | <b>detail</b>         |
| <b>Initial test load percentage</b>            | Percentage of the steady state load for the test.                                                                                                                                                                                                             | <b>detail</b>         |
| <b>Duration in seconds</b>                     | Period in seconds for which the test has been performed.                                                                                                                                                                                                      | <b>detail</b>         |
| <b>Test packet size</b>                        | Size of the test packet in bytes.                                                                                                                                                                                                                             | <b>detail</b>         |
| <b>Iteration</b>                               | Number of the test iteration.                                                                                                                                                                                                                                 | <b>detail</b>         |
| <b>Duration (sec)</b>                          | Period in seconds for which the test iteration is run.                                                                                                                                                                                                        | <b>detail</b>         |
| <b>Elapsed time</b>                            | Amount of time that has passed, in seconds, since the start of the test.                                                                                                                                                                                      | <b>detail</b>         |
| <b>pps</b>                                     | Total count of packets-per-second (pps) transmitted during the test.                                                                                                                                                                                          | <b>detail</b>         |
| <b>Tx Packets</b>                              | Number of transmitted test packets.                                                                                                                                                                                                                           | <b>detail</b>         |
| <b>Rx Packets</b>                              | Number of received test packets.                                                                                                                                                                                                                              | <b>detail</b>         |
| <b>Latency</b>                                 | Displays the latency parameters.                                                                                                                                                                                                                              | <b>detail</b>         |

Table 64: show services rpm rfc2544-benchmarking test-id Output Fields (*continued*)

| Field Name                                    | Field Description                                                                                           | Level of Output       |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>Min(ns)</b>                                | Aggregated minimum latency in nanoseconds.                                                                  | <b>detail</b>         |
| <b>Avg(ns)</b>                                | Aggregated average latency in nanoseconds.                                                                  | <b>detail</b>         |
| <b>Max(ns)</b>                                | Aggregated maximum latency in nanoseconds.                                                                  | <b>detail</b>         |
| <b>Probe(ns)</b>                              | Aggregated probe latency in nanoseconds.                                                                    | <b>detail</b>         |
| <b>Result of the iteration runs (Latency)</b> | Results of the latency test completed for a particular packet size.                                         | <b>detail</b>         |
| <b>Avg (min) Latency</b>                      | Average of the minimum latency in nanoseconds.                                                              | <b>detail</b>         |
| <b>Avg (avg) latency</b>                      | Average of the average latency in nanoseconds.                                                              | <b>detail</b>         |
| <b>Avg (Max) latency</b>                      | Average of the maximum latency in nanoseconds.                                                              | <b>detail</b>         |
| <b>Avg (probe) latency</b>                    | Average of the probe latency in nanoseconds.                                                                | <b>detail</b>         |
| <b>RFC2544 Latency test results summary:</b>  | Consolidated statistics of the latency test.                                                                | <b>detail summary</b> |
| <b>Packet Size</b>                            | Size of the test packet in bytes.                                                                           | <b>detail summary</b> |
| <b>Theoretical rate (pps)</b>                 | Theoretical frame rate in packets-per-second.                                                               | <b>detail summary</b> |
| <b>Tx Packets</b>                             | Number of transmitted packets.                                                                              | <b>detail summary</b> |
| <b>Rx Packets</b>                             | Number of received packets.                                                                                 | <b>detail summary</b> |
| <b>Latency</b>                                | Displays the latency parameters.                                                                            | <b>detail summary</b> |
| <b>Min(ns)</b>                                | Aggregated minimum latency in nanoseconds.                                                                  | <b>detail summary</b> |
| <b>Avg(ns)</b>                                | Aggregated average latency in nanoseconds.                                                                  | <b>detail summary</b> |
| <b>Max(ns)</b>                                | Aggregated maximum latency in nanoseconds.                                                                  | <b>detail summary</b> |
| <b>Probe(ns)</b>                              | Aggregated probe latency in nanoseconds.                                                                    | <b>detail summary</b> |
| <b>Rfc2544 Back-Back test information :</b>   | (ACX Series routers only) Details of the back-to-back frames or bursty frames test.                         | <b>detail</b>         |
| <b>Initial burst length:</b>                  | Length of the first burst when test frames are sent, as a measure of number of seconds at the rate of Kbps. | <b>detail</b>         |

Table 64: show services rpm rfc2544-benchmarking test-id Output Fields (*continued*)

| Field Name                                     | Field Description                                                                                                                                                          | Level of Output       |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>Test iteration mode :</b>                   | Mode of the test iteration: Binary or step-down.                                                                                                                           | <b>detail</b>         |
| <b>Test iteration step percent</b>             | The test step percentage for tests. If not specified, the default step-percent is 10 percent. This parameter is ignored for all type of tests other than frame-loss tests. | <b>detail</b>         |
| <b>Theoretical max bandwidth</b>               | The theoretical limit of the media for the frame size configured for the test. This value is typically set to the bandwidth of the server being tested.                    | <b>detail</b>         |
| <b>Test packet size:</b>                       | Packet size of the test frames in bytes.                                                                                                                                   | <b>detail</b>         |
| <b>Iteration</b>                               | Number of the test iteration.                                                                                                                                              | <b>detail</b>         |
| <b>Burst Length (Packets)</b>                  | Number of packets in the burst.                                                                                                                                            | <b>detail</b>         |
| <b>Elapsed time</b>                            | Amount of time that has passed, in seconds, since the start of the test.                                                                                                   | <b>detail</b>         |
| <b>Tx Packets</b>                              | Number of transmitted test packets.                                                                                                                                        | <b>detail</b>         |
| <b>Rx Packets</b>                              | Number of received test packets.                                                                                                                                           | <b>detail</b>         |
| <b>Tx Bytes</b>                                | Number of transmitted bytes.                                                                                                                                               | <b>detail</b>         |
| <b>Rx Bytes</b>                                | Number of received bytes.                                                                                                                                                  | <b>detail</b>         |
| <b>Result of the iteration runs :</b>          | Results of the back-to-back frames test completed for a certain packet size.                                                                                               | <b>detail</b>         |
| <b>Best iteration :</b>                        | Number of the iteration with the longest burst.                                                                                                                            | <b>detail</b>         |
| <b>Measured burst (num sec)</b>                | Time in seconds of the burst of the iteration with the longest burst.                                                                                                      | <b>detail</b>         |
| <b>Measured burst (num pkts)</b>               | Number of packets during the burst of the iteration with the longest burst.                                                                                                | <b>detail</b>         |
| <b>RFC2544 Back-Back test results summary:</b> | Consolidated statistics of the back-to-back frames test.                                                                                                                   | <b>detail summary</b> |
| <b>Packet Size</b>                             | Size of the test packets in bytes.                                                                                                                                         | <b>detail summary</b> |
| <b>Measure Burst length (Packets)</b>          | Computed burst length in terms of number of packets.                                                                                                                       | <b>detail summary</b> |



Table 64: show services rpm rfc2544-benchmarking test-id Output Fields (*continued*)

| Field Name                              | Field Description                                                                                                                                                          | Level of Output |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Rfc2544 frame-loss test information :   | (ACX Series routers only) Details of the frame-loss test.                                                                                                                  | detail          |
| Initial burst length:                   | Length of the first burst when test frames are sent, as a measure of number of seconds at the rate of Kbps.                                                                | detail          |
| Test iteration mode :                   | Mode of the test iteration: Binary or step-down.                                                                                                                           | detail          |
| Test iteration step percent             | The test step percentage for tests. If not specified, the default step-percent is 10 percent. This parameter is ignored for all type of tests other than frame-loss tests. | detail          |
| Theoretical max bandwidth               | The theoretical limit of the media for the frame size configured for the test. This value is typically set to the bandwidth of the server being tested.                    | detail          |
| Test packet size                        | Size of the test packets in bytes.                                                                                                                                         | detail          |
| Iteration                               | Number of the test iteration.                                                                                                                                              | detail          |
| Duration (sec)                          | Period, in seconds, for which the test iteration is run.                                                                                                                   | detail          |
| Offered throughput (percentage)         | The offered throughput in percentage of the chosen service (such as Layer 3 or Ethernet pseudowire)                                                                        | detail          |
| Elapsed time                            | Amount of time that has passed, in seconds, since the start of the test.                                                                                                   | detail          |
| pps                                     | Theoretical frame rate in packets-per-second.                                                                                                                              | detail          |
| Tx Packets                              | Number of transmitted test packets.                                                                                                                                        | detail          |
| Rx Packets                              | Number of received test packets.                                                                                                                                           | detail          |
| Tx Bytes                                | Number of transmitted bytes.                                                                                                                                               | detail          |
| Rx Bytes                                | Number of received bytes.                                                                                                                                                  | detail          |
| Frame-loss rate %                       | Percentage of frames that must been forwarded by the router under steady state (constant) load, but were not forwarded due to lack of resources.                           | detail          |
| Result of the iteration runs :          | Results of the frame-loss test completed for a certain packet size.                                                                                                        | detail          |
| Frame-loss rate (percent) :             | Percentage of dropped frames for the specified packet size                                                                                                                 | detail          |
| RFC2544 Frame-loss test results summary | Consolidated statistics of the frame-loss test                                                                                                                             | detail          |

Table 64: show services rpm rfc2544-benchmarking test-id Output Fields (*continued*)

| Field Name              | Field Description                                          | Level of Output |
|-------------------------|------------------------------------------------------------|-----------------|
| Packet Size             | Size of the test packet in bytes.                          | detail summary  |
| Theoretical rate (pps)  | Theoretical frame rate in packets-per-second.              | detail summary  |
| Percentage throughput   | Percentage of throughput for the test iteration.           | detail summary  |
| Tx Packets              | Number of transmitted packets.                             | detail summary  |
| Rx Packets              | Number of received packets.                                | detail summary  |
| Frame Loss rate percent | Percentage of dropped frames for the specified packet size | detail summary  |

## Sample Output

### show services rpm rfc2544-benchmarking test-id detail (Throughput Test on ACX Series routers )

```

user@host> show services rpm rfc2544-benchmarking test-id 19 detail
Test information :
 Test id: 19, Test name: test1, Test type: Throughput
 Test mode: Initiate-and-Terminate
 Test packet size: 64 1280
 Test state: RFC2544_TEST_STATE_COMPLETED
 Test start time: 2005-07-29 10:25:00 UTC
 Test finish time: 2005-07-29 10:26:02 UTC
 Counters last cleared: Never

Test-profile Configuration:
 Test-profile name: prof_tput
 Test packet size: 64 1280
 Therotical max bandwidth : 993000 kbps

Test Configuration:
 Test mode: Initiate-and-Terminate
 Duration in seconds: 20
 Test family: INET
 Routing Instance Name: default

Inet family Configuration:
 Egress Interface : ge-0/1/1.0
 Source ipv4 address: 20.6.0.1
 Destination ipv4 address: 20.6.0.2
 Source udp port: 2020
 Destination udp port: 3030

Rfc2544 throughput test information :
 Initial test load percentage : 100.00 %
 Test iteration mode : Binary
 Test iteration step percent : 50.00 %
 Therotical max bandwidth : 993000 kbps

```

```

Test packet size: 64
Iteration Duration Elapsed pps Tx Rx Tx Rx
Percentage
(sec) time Packets Packets Bytes Bytes
throughput
1 3 3 134918 404754 404754 27523272 27523272 10.00
%
2 20 20 1349184 26983501 26983501 1834878068 1834878068 100.00
%

```

Result of the iteration runs : Throughput Test complete for packet size 64  
 Best iteration : 2, Best iteration (pps) : 1349184  
 Best iteration throughput : 100.00 %

```

Test packet size: 1280
Iteration Duration Elapsed pps Tx Rx Tx Rx
Percentage
(sec) time Packets Packets Bytes Bytes
throughput
1 3 3 9489 28467 28467 36551628 36551628 10.00
%
2 20 20 94896 1897920 1897920 2436929280 2436929280 100.00
%

```

Result of the iteration runs : Throughput Test complete for packet size 1280  
 Best iteration : 2, Best iteration (pps) : 94896  
 Best iteration throughput : 100.00 %

RFC2544 Throughput test results summary:

| Packet Size | Theoretical rate (pps) | Tx Packets | Rx Packets | Offered throughput (percentage) | Measured bandwidth (kbps) |
|-------------|------------------------|------------|------------|---------------------------------|---------------------------|
| 64          | 1349184                | 26983501   | 26983501   | 100.00 %                        | 993000                    |
| 1280        | 94896                  | 1897920    | 1897920    | 100.00 %                        | 993000                    |

### show services rpm rfc2544-benchmarking test-id detail (Latency Test on ACX Series routers)

```
user@host> show services rpm rfc2544-benchmarking test-id 37 detail
```

Test information :

```

Test id: 37, Test name: test1, Test type: Latency
Test mode: Initiate-and-Terminate
Test packet size: 64 1280
Test state: RFC2544_TEST_STATE_COMPLETED
Test start time: 2005-07-29 10:26:41 UTC
Test finish time: 2005-07-29 10:36:15 UTC
Counters last cleared: Never

```

Test-profile Configuration:

```

Test-profile name: prof_latency
Test packet size: 64 1280
Theoretical max bandwidth : 993000 kbps

```

Test Configuration:

```

Test mode: Initiate-and-Terminate
Duration in seconds: 10
Test family: INET
Routing Instance Name: default

```

## Inet family Configuration:

Egress Interface : ge-0/1/1.0  
 Source ipv4 address: 20.6.0.1  
 Destination ipv4 address: 20.6.0.2  
 Source udp port: 2020  
 Destination udp port: 3030

## Rfc2544 latency test information :

Theoretical max bandwidth : 993000 kbps  
 Initial test load percentage : 100.00 %  
 Duration in seconds: 10

Test packet size: 64

| Iteration | Duration<br>(sec) | Elapsed<br>time | pps     | Tx<br>Packets | Rx<br>Packets |
|-----------|-------------------|-----------------|---------|---------------|---------------|
| 1         | 3                 | 3               | 134918  | 404754        | 404754        |
| 2         | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 3         | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 4         | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 5         | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 6         | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 7         | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 8         | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 9         | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 10        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 11        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 12        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 13        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 14        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 15        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 16        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 17        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 18        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 19        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 20        | 10                | 10              | 1349184 | 13491751      | 13491751      |
| 21        | 10                | 10              | 1349184 | 13491751      | 13491751      |

| ----- Latency ----- |         |         |           |
|---------------------|---------|---------|-----------|
| Min(ns)             | Avg(ns) | Max(ns) | Probe(ns) |
| 17464               | 18770   | 18880   | 18784     |
| 17472               | 18799   | 20488   | 18848     |
| 17472               | 18799   | 20416   | 18816     |
| 17472               | 18799   | 20440   | 18704     |
| 17464               | 18799   | 20376   | 18880     |
| 17464               | 18799   | 20232   | 18832     |
| 17464               | 18799   | 20400   | 18848     |
| 17472               | 18799   | 20240   | 18864     |
| 17472               | 18799   | 20264   | 18848     |
| 17464               | 18799   | 20264   | 18880     |
| 17472               | 18800   | 20320   | 18864     |
| 17464               | 18799   | 20176   | 18864     |
| 17464               | 18800   | 20248   | 18864     |
| 17464               | 18800   | 20272   | 18864     |
| 17464               | 18799   | 20472   | 18832     |
| 17464               | 18799   | 20256   | 18880     |
| 17464               | 18799   | 20336   | 18848     |
| 17464               | 18800   | 20688   | 18848     |
| 17472               | 18800   | 20504   | 18864     |
| 17464               | 18799   | 20448   | 18768     |
| 17472               | 18799   | 20240   | 18864     |

Result of the iteration runs : Latency Test complete for packet size 64

Avg (min) Latency : 17466  
 Avg (avg) latency : 18799  
 Avg (Max) latency : 20360  
 Avg (probe) latency : 18844

Test packet size: 1280

| Iteration | Duration<br>(sec) | Elapsed<br>time | pps   | Tx<br>Packets | Rx<br>Packets |
|-----------|-------------------|-----------------|-------|---------------|---------------|
| 1         | 3                 | 3               | 9489  | 28467         | 28467         |
| 2         | 10                | 10              | 94896 | 948960        | 948960        |
| 3         | 10                | 10              | 94896 | 948960        | 948960        |
| 4         | 10                | 10              | 94896 | 948960        | 948960        |
| 5         | 10                | 10              | 94896 | 948960        | 948960        |
| 6         | 10                | 10              | 94896 | 948960        | 948960        |
| 7         | 10                | 10              | 94896 | 948960        | 948960        |
| 8         | 10                | 10              | 94896 | 948960        | 948960        |
| 9         | 10                | 10              | 94896 | 948960        | 948960        |
| 10        | 10                | 10              | 94896 | 948960        | 948960        |
| 11        | 10                | 10              | 94896 | 948960        | 948960        |
| 12        | 10                | 10              | 94896 | 948960        | 948960        |
| 13        | 10                | 10              | 94896 | 948960        | 948960        |
| 14        | 10                | 10              | 94896 | 948960        | 948960        |
| 15        | 10                | 10              | 94896 | 948960        | 948960        |
| 16        | 10                | 10              | 94896 | 948960        | 948960        |
| 17        | 10                | 10              | 94896 | 948960        | 948960        |
| 18        | 10                | 10              | 94896 | 948960        | 948960        |
| 19        | 10                | 10              | 94896 | 948960        | 948960        |
| 20        | 10                | 10              | 94896 | 948960        | 948960        |
| 21        | 10                | 10              | 94896 | 948960        | 948960        |

----- Latency -----

| Min(ns) | Avg(ns) | Max(ns) | Probe(ns) |
|---------|---------|---------|-----------|
| 68712   | 70031   | 70576   | 69456     |
| 68728   | 70344   | 71808   | 70512     |
| 68720   | 70344   | 71744   | 70352     |
| 68720   | 70344   | 71680   | 70112     |
| 68720   | 70345   | 71856   | 70352     |
| 68720   | 70344   | 71808   | 70384     |
| 68720   | 70344   | 71752   | 70480     |
| 68720   | 70344   | 71880   | 70112     |
| 68720   | 70344   | 71792   | 70320     |
| 68728   | 70345   | 73344   | 70336     |
| 68720   | 70344   | 71688   | 70560     |
| 68728   | 70345   | 71896   | 70496     |
| 68720   | 70344   | 71760   | 70096     |
| 68720   | 70344   | 71776   | 70320     |
| 68720   | 70344   | 71760   | 70400     |
| 68712   | 70345   | 71920   | 70352     |
| 68720   | 70344   | 71792   | 70576     |
| 68720   | 70345   | 71840   | 70320     |
| 68720   | 70344   | 71792   | 70368     |
| 68720   | 70345   | 71824   | 70464     |
| 68712   | 70345   | 71904   | 70512     |

Result of the iteration runs : Latency Test complete for packet size 1280

Avg (min) Latency : 68720  
 Avg (avg) latency : 70344

```

Avg (Max) latency : 71880
Avg (probe) latency : 70371

```

```

RFC2544 Latency test results summary:

```

| Packet Size | Theoretical rate (pps) | Tx Packets | Rx Packets | ----- Latency ----- |         |         |           |
|-------------|------------------------|------------|------------|---------------------|---------|---------|-----------|
|             |                        |            |            | Min(ns)             | Avg(ns) | Max(ns) | Probe(ns) |
| 64          | 1349184                | 269835020  | 269835020  | 17466               | 18799   | 20360   | 18844     |
| 1280        | 94896                  | 18979200   | 18979200   | 68720               | 70344   | 71880   | 70371     |

### show services rpm rfc2544-benchmarking test-id detail (Frame Loss Test on ACX Series routers)

```

user@host> show services rpm rfc2544-benchmarking test-id 73 detail

```

```

Test information :

```

```

Test id: 73, Test name: test1, Test type: Frame-Loss
Test mode: Initiate-and-Terminate
Test packet size: 64 1280
Test state: RFC2544_TEST_STATE_COMPLETED
Test start time: 2005-07-29 10:38:41 UTC
Test finish time: 2005-07-29 10:41:19 UTC
Counters last cleared: Never

```

```

Test-profile Configuration:

```

```

Test-profile name: prof_fl
Test packet size: 64 1280
Theoretical max bandwidth : 993000 kbps

```

```

Test Configuration:

```

```

Test mode: Initiate-and-Terminate
Duration in seconds: 20
Test family: INET
Routing Instance Name: default

```

```

Inet family Configuration:

```

```

Egress Interface : ge-0/1/1.0
Source ipv4 address: 20.6.0.1
Destination ipv4 address: 20.6.0.2
Source udp port: 2020
Destination udp port: 3030

```

```

Rfc2544 frame-loss test information :

```

```

Initial test load percentage : 100.00 %
Test iteration mode : step-down
Test iteration step percent : 10 %
Theoretical max bandwidth : 993000 kbps

```

```

Test packet size: 64

```

| Iteration  | Duration | Elapsed | Offered     | pps     | Tx       | Rx       | Tx         | Rx    |
|------------|----------|---------|-------------|---------|----------|----------|------------|-------|
| Frame-loss |          |         |             |         |          |          |            |       |
|            | (sec)    | time    | throughput% |         | Packets  | Packets  | Bytes      | Bytes |
| rate %     |          |         |             |         |          |          |            |       |
| 1          | 3        | 3       | 10.00 %     | 134918  | 404754   | 404754   | 27523272   |       |
| 27523272   | 0.00 %   |         |             |         |          |          |            |       |
| 2          | 20       | 20      | 100.00 %    | 1349184 | 26983501 | 26983501 | 1834878068 |       |
| 1834878068 | 0.00 %   |         |             |         |          |          |            |       |
| 3          | 20       | 20      | 100.00 %    | 1349184 | 26983501 | 26983501 | 1834878068 |       |
| 1834878068 | 0.00 %   |         |             |         |          |          |            |       |
| 4          | 20       | 20      | 100.00 %    | 1349184 | 26983501 | 26983501 | 1834878068 |       |
| 1834878068 | 0.00 %   |         |             |         |          |          |            |       |

Result of the iteration runs : Frame-loss test complete for packet size 64  
 Frame-loss rate (percent) : 0.00 %

Test packet size: 1280

| Iteration | Duration<br>Frame-loss<br>(sec) | Elapsed<br>time | Offered<br>throughput% | pps   | Tx<br>Packets | Rx<br>Packets | Tx<br>Bytes | Rx<br>Bytes |
|-----------|---------------------------------|-----------------|------------------------|-------|---------------|---------------|-------------|-------------|
| 1         | 3                               | 3               | 10.00 %                | 9489  | 404754        | 28467         | 36551628    |             |
| 2         | 20                              | 20              | 100.00 %               | 94896 | 1897920       | 1897920       | 2436929280  |             |
| 3         | 20                              | 20              | 100.00 %               | 94896 | 1897920       | 1897920       | 2436929280  |             |
| 4         | 20                              | 20              | 100.00 %               | 94896 | 1897920       | 1897920       | 2436929280  |             |

Result of the iteration runs : Frame-loss test complete for packet size 1280  
 Frame-loss rate (percent) : 0.00 %

RFC2544 Frame-loss test results summary:

| Packet<br>Loss<br>Size<br>percent | Theoretical<br>rate (pps) | Percentage<br>throughput | Tx<br>Packets | Rx<br>Packets | Frame<br>rate |
|-----------------------------------|---------------------------|--------------------------|---------------|---------------|---------------|
| 64                                | 1349184                   | 100.00 %                 | 26983501      | 26983501      | 0.00          |
| 1280                              | 94896                     | 100.00 %                 | 1897920       | 1897920       | 0.00          |

#### show services rpm rfc2544-benchmarking test-id detail (Back-to-Back Frames Test on ACX Series routers)

user@host> show services rpm rfc2544-benchmarking test-id 55 detail

Test information :

Test id: 55, Test name: test1, Test type: Back-Back-Frames  
 Test mode: Initiate-and-Terminate  
 Test packet size: 64 1280  
 Test state: RFC2544\_TEST\_STATE\_COMPLETED  
 Test start time: 2005-07-29 10:36:54 UTC  
 Test finish time: 2005-07-29 10:37:57 UTC  
 Counters last cleared: Never

Test-profile Configuration:

Test-profile name: prof\_b2b  
 Test packet size: 64 1280  
 Therotical max bandwidth : 993000 kbps

Test Configuration:

Test mode: Initiate-and-Terminate  
 Duration in seconds: 20  
 Test family: INET  
 Routing Instance Name: default

```
Inet family Configuration:
 Egress Interface : ge-0/1/1.0
 Source ipv4 address: 20.6.0.1
 Destination ipv4 address: 20.6.0.2
 Source udp port: 2020
 Destination udp port: 3030
```

```
Rfc2544 Back-Back test information :
 Initial burst length: 20 seconds at 993000 kbps
 Test iteration mode : Binary
 Test iteration step percent : 50.00 %
```

```
Test packet size: 64
Iteration Burst Length Elapsed Tx Rx Tx
 Rx time Packets Packets Bytes
 (Packets)
 Bytes
1 404754 3 404754 404754 27523272
27523272
2 26983680 20 26983680 26983680 1834890240
1834890240
```

```
Result of the iteration runs : Back-Back-Frames Test complete for packet size
64
```

```
Best iteration : 2
Measured burst (num sec) : 20 sec,
Measured burst (num pkts) : 26983680 packets
Result of the iteration runs : Back-Back-Frames Test complete for packet size
64
```

```
Best iteration : 2
Measured burst (num sec) : 20 sec,
Measured burst (num pkts) : 26983680 packets
```

```
Test packet size: 1280
Iteration Burst Length Elapsed Tx Rx Tx
 Rx time Packets Packets Bytes
 (Packets)
 Bytes
1 28467 3 28467 28467 36551628
36551628
2 1897920 20 1897920 1897920 2436929280
2436929280
```

```
Result of the iteration runs : Back-Back-Frames Test complete for packet size
12
```

```
Best iteration : 2
Measured burst (num sec) : 20 sec,
Measured burst (num pkts) : 1897920 packets
```

```
RFC2544 Back-Back test results summary:
```

```

Packet Measure Burst
Size length (Packets)
64 26983680 packets
1280 1897920 packets
```

**show services rpm rfc2544-benchmarking test-id detail (Reflection Test on MX104 routers)**

```
user@host> show services rpm rfc2544-benchmarking test-id detail 1
```



```
Test information :
 Test id: 1, Test name: fort_uni_inet_ref, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: RFC2544_TEST_STATE_RUNNING
 Status: Running
 Test start time: 2013-12-09 16:24:52 IST
 Test finish time: TEST_RUNNING
 Counters last cleared: Never
```

```
Test Configuration:
 Test mode: Reflect
 Duration in seconds: 864000
 Test family: INET
 Routing Instance Name: default
```

```
Inet family Configuration:
 Egress Interface : ge-0/3/1.0
 Destination ipv4 address: 21.1.1.2
 Destination udp port: 200
```

| Elapsed<br>time | Reflected<br>Packets | Reflected<br>Bytes |
|-----------------|----------------------|--------------------|
| 176             | 8977917              | 9031784502         |

#### show services rpm rfc2544-benchmarking test-id brief (Reflection Test on MX104 routers)

```
user@host> show services rpm rfc2544-benchmarking test-id brief 1
Test information :
 Test id: 1, Test name: fort_uni_inet_ref, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: RFC2544_TEST_STATE_RUNNING
 Status: Running
 Test start time: 2013-12-09 16:24:52 IST
 Test finish time: TEST_RUNNING
 Counters last cleared: Never
```

#### show services rpm rfc2544-benchmarking test-id detail (Reflection Test on MX104 routers)

```
user@host> show services rpm rfc2544-benchmarking test-id detail 2
Test information :
 Test id: 2, Test name: fort_uni_inet_ref, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: RFC2544_TEST_STATE_RUNNING
 Status: Running
 Test start time: 2013-12-09 16:39:18 IST
 Test finish time: TEST_RUNNING
 Counters last cleared: Never

Test Configuration:
 Test mode: Reflect
 Duration in seconds: 864000
 Test family: CCC
 Routing Instance Name: default

CCC family Configuration:
 Interface : ge-0/3/2.0
 Test direction: Egress
```

| Elapsed<br>time | Reflected<br>Packets | Reflected<br>Bytes |
|-----------------|----------------------|--------------------|
| 23              | 809137               | 825319740          |

**show services rpm rfc2544-benchmarking test-id brief (Reflection Test on MX104 routers)**

```
user@host> show services rpm rfc2544-benchmarking test-id 2 brief
Test information :
 Test id: 2, Test name: fort_uni_inet_ref, Test type: Reflect
 Test mode: Reflect
 Test packet size: 0
 Test state: RFC2544_TEST_STATE_RUNNING
 Status: Running
 Test start time: 2013-12-09 16:39:18 IST
 Test finish time: TEST_RUNNING
 Counters last cleared: Never
```

## show services rpm twamp client connection

|                                 |                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show services rpm twamp client connection</b><br><i>&lt;connection-name&gt;</i>                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 15.1 for MX Series routers.                                                                                                                                                                                                                                            |
| <b>Description</b>              | Display information about the connections established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control-clients. By default, all established sessions are displayed, unless you specify a control-connection name when you issue the command. |
| <b>Options</b>                  | <i>connection-name</i> —(Optional) Display information about the specified control-connection or TWAMP control-client.                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">show services rpm twamp client connection on page 657</a>                                                                                                                                                                                                                                         |
| <b>Output Fields</b>            | <a href="#">Table 65 on page 657</a> lists the output fields for the <b>show services rpm twamp client connection</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                        |

**Table 65: show services rpm twamp client connection Output Fields**

| Field Name      | Field Description                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------|
| Connection Name | Connection name that uniquely identifies the connection between the TWAMP server and a particular client. |
| Client address  | Client IP address.                                                                                        |
| Client port     | Client port number.                                                                                       |
| Server address  | Server IP address.                                                                                        |
| Server port     | Server port number.                                                                                       |
| Session count   | Session count.                                                                                            |
| Auth mode       | Authentication mode.                                                                                      |

## Sample Output

### show services rpm twamp client connection

```

user@host> show services rpm twamp client connection
 Connection Client Client Server Server Session Auth
 ID address port address port count mode

```

|               |     |                 |       |                 |       |    |      |
|---------------|-----|-----------------|-------|-----------------|-------|----|------|
|               | 4   | 1.1.1.1         | 12345 | 192.168.219.203 | 890   | 16 | none |
|               | 78  | 3.22.1.55       | 345   | 22.2.2.2        | 89022 | 5  | none |
|               | 234 | 192.168.219.203 | 2345  | 2.2.22.2        | 3333  | 16 | none |
| authenticated | 5   | 221.4.1.1       | 82345 | 2.2.2.2         | 45909 | 16 |      |
| encrypted     | 1   | 192.168.1.1     | 645   | 32.2.2.23       | 2394  | 16 |      |

## show services rpm twamp client history-results

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show services rpm history-results &lt;brief   detail&gt; &lt;control-connection <i>control-connection-name</i>&gt; &lt;since <i>time</i>&gt; &lt;test-session <i>test-session-name</i>&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 15.1 for MX Series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Display standard information about the results of the last 50 probes for each real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) instance. You can also view the historical results of the probes or test packets sent from a TWAMP client to a TWAMP server for a particular control-connection, or a test-session associated with a control-connection.                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>                  | <p><b>none</b>—Display the results of the last 50 probes for all RPM TWAMP instances.</p> <p><b>brief   detail</b>—(Optional) Display the specified level of output.</p> <p><b>control-connection <i>control-connection-name</i></b>—(Optional) Display information for the specified control-connection between a TWAMP client and a TWAMP server.</p> <p><b>since <i>time</i></b>—(Optional) Display information from the specified time. Specify time as <i>yyyy-mm-dd.hh:mm:ss</i>.</p> <p><b>test-session <i>test-session-name</i></b>—(Optional) Display information for the specified test session associated with a control-connection between a TWAMP client and a TWAMP server.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <p><a href="#">show services rpm twamp client history-results on page 660</a></p> <p><a href="#">show services rpm twamp client history-results detail on page 661</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Output Fields</b>            | <a href="#">Table 61 on page 625</a> lists the output fields for the <b>show services rpm twamp client history-results</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 66: show services rpm twamp client history-results Output Fields

| Field Name             | Field Description                                    | Level of Output |
|------------------------|------------------------------------------------------|-----------------|
| <b>Owner</b>           | Probe owner or the TWAMP client.                     | All levels      |
| <b>Test</b>            | Name of a test for a TWAMP probe instance.           | All levels      |
| <b>Probe received</b>  | Timestamp when the probe result was determined.      | All levels      |
| <b>Round trip time</b> | Average ping round-trip time (RTT), in microseconds. | All levels      |

Table 66: show services rpm twamp client history-results Output Fields (*continued*)

| Field Name                       | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Level of Output |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Probe results</b>             | Result of a particular probe performed by a remote host. The following information is contained in the results: <ul style="list-style-type: none"> <li>• <b>Response received</b>—Timestamp when the probe result was determined.</li> <li>• <b>Rtt</b>—Average ping round-trip time (RTT), in microseconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail</b>   |
| <b>Results over current test</b> | Displays the results for the current test by probe at the time each probe was completed, as well as the status of the current test at the time the probe was completed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail</b>   |
| <b>Probes sent</b>               | Number of probes sent with the current test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>detail</b>   |
| <b>Probes received</b>           | Number of probe responses received within the current test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>detail</b>   |
| <b>Loss percentage</b>           | Percentage of lost probes for the current test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>detail</b>   |
| <b>Measurement</b>               | Increment of measurement. Possible values are round-trip time delay and, for the probe type icmp-ping-timestamp, the egress and ingress delay: <ul style="list-style-type: none"> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Peak to peak</b>—Difference between two peak values of RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Jitter</b>—Difference, in microseconds, between the maximum and minimum RTT measured over the course of the current test.</li> <li>• <b>Sum</b>—Total round-trip time, in microseconds, measured over the course of the current test.</li> </ul> | <b>detail</b>   |

## Sample Output

### show services rpm twamp client history-results

```

user@host> show services rpm twamp client history-results
Owner, Test Probe received Round trip time
c2, t1 Fri Feb 13 00:31:54 2015 Request timed out
c2, t1 Fri Feb 13 00:31:55 2015 Request timed out
c2, t1 Fri Feb 13 00:31:56 2015 Request timed out
c2, t1 Fri Feb 13 00:31:57 2015 Request timed out
c2, t1 Fri Feb 13 00:31:58 2015 Request timed out
c2, t1 Fri Feb 13 00:31:59 2015 Request timed out
c2, t1 Fri Feb 13 00:32:00 2015 Request timed out
c2, t1 Fri Feb 13 00:32:01 2015 Request timed out
c2, t1 Fri Feb 13 00:32:02 2015 Request timed out
c2, t1 Fri Feb 13 00:32:03 2015 Request timed out
c2, t1 Fri Feb 13 00:32:04 2015 Request timed out
c2, t1 Fri Feb 13 00:32:05 2015 Request timed out
c2, t1 Fri Feb 13 00:32:06 2015 Request timed out
c2, t1 Fri Feb 13 00:32:07 2015 Request timed out

```

```

c2, t1 Fri Feb 13 00:32:08 2015 Request timed out
c2, t1 Fri Feb 13 00:32:09 2015 Request timed out
c2, t1 Fri Feb 13 00:32:10 2015 Request timed out
c2, t1 Fri Feb 13 00:32:11 2015 Request timed out
c2, t1 Fri Feb 13 00:32:12 2015 Request timed out
c2, t1 Fri Feb 13 00:32:13 2015 Request timed out
c2, t1 Fri Feb 13 00:32:14 2015 Request timed out
c2, t1 Fri Feb 13 00:32:15 2015 Request timed out
c2, t1 Fri Feb 13 00:32:16 2015 Request timed out
c2, t1 Fri Feb 13 00:32:17 2015 Request timed out
c2, t1 Fri Feb 13 00:32:18 2015 Request timed out
c2, t1 Fri Feb 13 00:32:19 2015 Request timed out
c2, t1 Fri Feb 13 00:32:20 2015 Request timed out
c2, t1 Fri Feb 13 00:32:21 2015 Request timed out
c2, t1 Fri Feb 13 00:32:22 2015 Request timed out
c2, t1 Fri Feb 13 00:32:23 2015 Request timed out
c2, t1 Fri Feb 13 00:32:24 2015 Request timed out
c2, t1 Fri Feb 13 00:32:25 2015 Request timed out
c2, t1 Fri Feb 13 00:32:26 2015 Request timed out
c2, t1 Fri Feb 13 00:32:27 2015 Request timed out
c2, t1 Fri Feb 13 00:32:28 2015 Request timed out
c2, t1 Fri Feb 13 00:32:29 2015 Request timed out
c2, t1 Fri Feb 13 00:32:30 2015 Request timed out
c2, t1 Fri Feb 13 00:32:31 2015 Request timed out
c2, t1 Fri Feb 13 00:32:32 2015 Request timed out
c2, t1 Fri Feb 13 00:32:33 2015 Request timed out
c2, t1 Fri Feb 13 00:32:34 2015 Request timed out
c2, t1 Fri Feb 13 00:32:35 2015 Request timed out
c2, t1 Fri Feb 13 00:32:36 2015 Request timed out
c2, t1 Fri Feb 13 00:32:37 2015 Request timed out
c2, t1 Fri Feb 13 00:32:38 2015 Request timed out
c2, t1 Fri Feb 13 00:32:39 2015 Request timed out
c2, t1 Fri Feb 13 00:32:40 2015 Request timed out
c2, t1 Fri Feb 13 00:32:41 2015 Request timed out
c2, t1 Fri Feb 13 00:32:42 2015 Request timed out
c2, t1 Fri Feb 13 00:32:43 2015 Request timed out

p1, t1 Wed Aug 12 01:02:42 2009 1180 usec

```

#### show services rpm twamp client history-results detail

```

user@host> show services rpm twamp-client history-results detail
Owner: p, Test: t
Probe results:
 Response received, Tue Jan 7 05:11:49 2014,
 Rtt: 184 usec, Round trip jitter: -96 usec, Round trip interarrival jitter:
57 usec
Results over current test:
 Probes sent: 4, Probes received: 4, Loss percentage: 0
 Measurement: Round trip time
 Samples: 4, Minimum: 174 usec, Maximum: 196 usec, Average: 183 usec, Peak
to peak: 22 usec, Stddev: 8 usec, Sum: 732 usec
 Measurement: Positive round trip jitter
 Samples: 1, Minimum: 110 usec, Maximum: 110 usec, Average: 110 usec, Peak
to peak: 0 usec, Stddev: 0 usec, Sum: 110 usec
 Measurement: Negative round trip jitter
 Samples: 2, Minimum: 96 usec, Maximum: 811 usec, Average: 454 usec, Peak
to peak: 715 usec, Stddev: 358 usec, Sum: 907 usec

Owner: p, Test: t

```

Probe results:  
Response received, Tue Jan 7 05:11:50 2014, Rtt: 174 usec, Round trip jitter: -8 usec, Round trip interarrival jitter: 54 usec  
Results over current test:  
Probes sent: 5, Probes received: 5, Loss percentage: 0  
Measurement: Round trip time  
Samples: 5, Minimum: 174 usec, Maximum: 196 usec, Average: 181 usec, Peak to peak: 22 usec, Stddev: 8 usec, Sum: 906 usec  
Measurement: Positive round trip jitter  
Samples: 1, Minimum: 110 usec, Maximum: 110 usec, Average: 110 usec, Peak to peak: 0 usec, Stddev: 0 usec, Sum: 110 usec  
Measurement: Negative round trip jitter  
Samples: 3, Minimum: 8 usec, Maximum: 811 usec, Average: 305 usec, Peak to peak: 803 usec, Stddev: 360 usec, Sum: 915 usec



## show services rpm twamp client probe-results

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services rpm twamp client probe-results<br><control-connection <i>control-connection-name</i> ><br><test-session <i>test-session-name</i> >                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 15.1 for MX Series routers.                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Display the results of the most recent real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) probes sent from the TWAMP client to the TWAMP server. You can also view the results of the probes or test packets sent from a TWAMP client to a TWAMP server for a particular control-connection, or a test-session associated with a control-connection.                                                                     |
| <b>Options</b>                  | <p><b>none</b>—Display all results of the most recent TWAMP probes.</p> <p><b>control-connection <i>control-connection-name</i></b>—(Optional) Display information for the specified control-connection between a TWAMP client and a TWAMP server.</p> <p><b>test-session <i>test-session-name</i></b>—(Optional) Display information for the specified test session associated with a control-connection between a TWAMP client and a TWAMP server.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>List of Sample Output</b>    | <a href="#">show services rpm twamp client probe-results on page 666</a><br><a href="#">show services rpm twamp client probe-results on page 666</a>                                                                                                                                                                                                                                                                                                     |
| <b>Output Fields</b>            | Table 67 on page 663 lists the output fields for the <b>show services twamp client probe-results</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                    |

Table 67: show services twamp client probe-results Output Fields

| Field Name               | Field Description                                                                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Owner</b>             | Name of the session-sender or the control-client, which is the TWAMP client. When you configure the <b>control-client-name</b> option at the <b>[edit services twamp client control-connection]</b> hierarchy level, this field displays the configured owner name or the client name. |
| <b>Test</b>              | Name of a test representing a collection of probes. When you configure the <b>test-session test-name</b> statement at the <b>[edit services owner]</b> hierarchy level, the field displays the configured test name.                                                                   |
| <b>server-address</b>    | Destination address used for the probes.                                                                                                                                                                                                                                               |
| <b>server-port</b>       | Destination port used for the probes.                                                                                                                                                                                                                                                  |
| <b>Client address</b>    | Source or TWAMP client address used for the probes.                                                                                                                                                                                                                                    |
| <b>Client port</b>       | Source or TWAMP client port used for the probes.                                                                                                                                                                                                                                       |
| <b>Reflector address</b> | Session-reflector or TWAMP server address used for the probes.                                                                                                                                                                                                                         |

Table 67: show services twamp client probe-results Output Fields (*continued*)

| Field Name                        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reflector port</b>             | Session-reflector or TWAMP server port used for the probes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Probe type</b>                 | Protocol configured on the receiving probe server: <b>http-get</b> , <b>http-metadata-get</b> , <b>icmp-ping</b> , <b>icmp-ping-timestamp</b> , <b>tcp-ping</b> , <b>udp-ping</b> , or <b>udp-ping-timestamp</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Test size</b>                  | Number of probes within a test.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Destination Interface Name</b> | Name of the interface configured on the TWAMP server or the session-reflector on which the TWAMP probe packets sent from the TWAMP client are received.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Probe results</b>              | <p>Raw measurement of a particular probe sample done by a remote host. This data is provided separately from the calculated results. The following information is contained in the raw measurement:</p> <ul style="list-style-type: none"> <li>• <b>Response received</b>—Timestamp when the probe result was determined.</li> <li>• <b>Client and server hardware timestamps</b>—If timestamps are configured, an entry appears at this point.</li> <li>• <b>Rtt</b>—Average ping round-trip time (RTT), in microseconds.</li> <li>• <b>Egress jitter</b>—Egress jitter, in microseconds.</li> <li>• <b>Ingress jitter</b>—Ingress jitter, in microseconds.</li> <li>• <b>Round trip jitter</b>—Round-trip jitter, in microseconds.</li> <li>• <b>Egress interarrival jitter</b>—Egress interarrival jitter, in microseconds.</li> <li>• <b>Ingress interarrival jitter</b>—Ingress interarrival jitter, in microseconds.</li> <li>• <b>Round trip interarrival jitter</b>—Round-trip interarrival jitter, in microseconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Results over current test</b>  | <p>Probes are grouped into tests, and the statistics are calculated for each test. If a test contains 10 probes, the average, minimum, and maximum results are calculated from the results of those 10 probes. If the command is issued while the test is in progress, the statistics use information from the completed probes.</p> <ul style="list-style-type: none"> <li>• <b>Probes sent</b>—Number of probes sent within the current test.</li> <li>• <b>Probes received</b>—Number of probe responses received within the current test.</li> <li>• <b>Loss percentage</b>—Percentage of lost probes for the current test.</li> <li>• <b>Measurement</b>—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type <b>icmp-ping-timestamp</b>, the egress delay and ingress delay.</li> </ul> <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> <li>• <b>Samples</b>—Number of probes.</li> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Peak to peak</b>—Peak-to-peak difference, in microseconds.</li> <li>• <b>Stddev</b>—Standard deviation, in microseconds.</li> <li>• <b>Sum</b>—Statistical sum.</li> </ul> |

Table 67: show services twamp client probe-results Output Fields (*continued*)

| Field Name                    | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Results over last test</b> | <p>Results for the most recently completed test. If the command is issued while the first test is in progress, this information is not displayed</p> <ul style="list-style-type: none"> <li>• <b>Probes sent</b>—Number of probes sent for the most recently completed test.</li> <li>• <b>Probes received</b>—Number of probe responses received for the most recently completed test.</li> <li>• <b>Loss percentage</b>—Percentage of lost probes for the most recently completed test.</li> <li>• <b>Test completed</b>—Time the most recent test was completed.</li> <li>• <b>Measurement</b>—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type <b>icmp-ping-timestamp</b>, the egress delay and ingress delay.</li> </ul> <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> <li>• <b>Samples</b>—Number of probes.</li> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured for the most recently completed test.</li> <li>• <b>Peak to peak</b>—Peak-to-peak difference, in microseconds.</li> <li>• <b>Stddev</b>—Standard deviation, in microseconds.</li> <li>• <b>Sum</b>—Statistical sum.</li> </ul> |
| <b>Results over all tests</b> | <p>Displays statistics made for all the probes, independently of the grouping into tests, as well as statistics for the current test.</p> <ul style="list-style-type: none"> <li>• <b>Probes sent</b>—Number of probes sent in all tests.</li> <li>• <b>Probes received</b>—Number of probe responses received in all tests.</li> <li>• <b>Loss percentage</b>—Percentage of lost probes in all tests.</li> <li>• <b>Measurement</b>—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe types <b>icmp-ping-timestamp</b> and <b>udp-ping-timestamp</b>, the egress delay and ingress delay.</li> </ul> <p>For each measurement type, the following individual calculated results are provided:</p> <ul style="list-style-type: none"> <li>• <b>Samples</b>—Number of probes.</li> <li>• <b>Minimum</b>—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Maximum</b>—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Average</b>—Average RTT, ingress delay, or egress delay measured over the course of the current test.</li> <li>• <b>Peak to peak</b>—Peak-to-peak difference, in microseconds.</li> <li>• <b>Stddev</b>—Standard deviation, in microseconds.</li> <li>• <b>Sum</b>—Statistical sum.</li> </ul>                                                                                                                                  |

## Sample Output

### show services rpm twamp client probe-results

```
user@host> show services rpm twamp client probe-results
Owner: c2, Test: t1
server-address: 13.13.13.14, server-port: 862, Client address: 13.13.13.13,
Client port: 57170
Reflector address: 13.13.13.14, Reflector port: 10011,
Sender address: 13.13.13.13, sender-port: 10011
Destination interface name: si-1/1/0.10
Test size: 500 probes
Probe results:
 Request timed out, Fri Feb 13 00:18:29 2015
Results over current test:
 Probes sent: 349, Probes received: 0, Loss percentage: 100.00000
Results over last test:
 Probes sent: 500, Probes received: 0, Loss percentage: 100.00000
Results over all tests:
 Probes sent: 4349, Probes received: 0, Loss percentage: 100.00000
```

### show services rpm twamp client probe-results

```
user@host> show services rpm twamp client probe-results control-connection c2
Owner: c2, Test: t1
server-address: 13.13.13.14, server-port: 862, Client address: 13.13.13.13,
Client port: 57170
Reflector address: 13.13.13.14, Reflector port: 10010,
Sender address: 13.13.13.13, sender-port: 10010
Destination interface name: si-1/1/0.10
Test size: 500 probes
Probe results:
 Request timed out, Fri Feb 13 00:07:14 2015
Results over current test:
 Probes sent: 188, Probes received: 0, Loss percentage: 100.00000
Results over last test:
 Probes sent: 500, Probes received: 0, Loss percentage: 100.00000
Results over all tests:
 Probes sent: 3688, Probes received: 0, Loss percentage: 100.00000
```

## show services rpm twamp client session

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show services rpm twamp client session</b><br><code>&lt;control-connection control-connection-name&gt;</code><br><code>&lt;test-session test-session-name&gt;</code>                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 15.1 for MX Series routers.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Display information about the sessions established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control clients for control packets and data packets. By default, all established control-connection and data-connection or test sessions are displayed, unless you specify a control-connection name or a test-session name when you issue the command.                           |
| <b>Options</b>                  | <p><b>control-connection-name</b>—(Optional) Display information about the specified control-connection, which is established for control-packets exchanged between a TWAMP client and a TWAMP server.</p> <p><b>test-session-name</b>—(Optional) Display information about the specified test session, which is established for data packets transmitted between a TWAMP client and a TWAMP server, associated with a control-connection..</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>List of Sample Output</b>    | <a href="#">show services rpm twamp client session on page 668</a><br><a href="#">show services rpm twamp client session on page 668</a>                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | <a href="#">Table 68 on page 667</a> lists the output fields for the <b>show services rpm twamp client session</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                             |

**Table 68: show services rpm twamp client session Output Fields**

| Field Name               | Field Description                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Connection Name</b>   | Name of the control connection that uniquely identifies the connection between the TWAMP server and the TWAMP client. |
| <b>Session Name</b>      | Name of the test session that uniquely identifies the data-session between the TWAMP server and the TWAMP client.     |
| <b>Sender address</b>    | Sender IP address.                                                                                                    |
| <b>Sender port</b>       | Sender port number.                                                                                                   |
| <b>Reflector address</b> | Reflector IP address.                                                                                                 |
| <b>Reflector port</b>    | Reflector port number.                                                                                                |

## Sample Output

### show services rpm twamp client session

```
user@host> show services rpm twamp client session
```

| Connection<br>Name | Session<br>Name | Sender<br>address | Sender<br>port | Reflector<br>address | Reflector<br>port |
|--------------------|-----------------|-------------------|----------------|----------------------|-------------------|
| cs1                | ts1             | 9.9.9.1           | 41998          | 9.9.9.2              | 5008              |
| cs2                | ts1             | 9.9.9.1           | 53710          | 9.9.9.2              | 5009              |

## Sample Output

### show services rpm twamp client session

```
user@host> show services rpm twamp client session control-connection c2
```

| Connection<br>Name | Session<br>Name | Sender<br>address | Sender<br>port | Reflector<br>address | Reflector<br>port |
|--------------------|-----------------|-------------------|----------------|----------------------|-------------------|
| c2                 | t1              | 13.13.13.13       | 10008          | 13.13.13.14          | 10008             |

## show services rpm twamp server connection

|                                 |                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show services rpm twamp server connection</b><br><i>&lt;connection-id&gt;</i>                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                      |
| <b>Description</b>              | Display information about the connections established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control-clients. By default, all established sessions are displayed, unless you specify a session ID when you issue the command. |
| <b>Options</b>                  | <i>connection-id</i> —(Optional) Display only information about the specified connection ID.                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                             |
| <b>List of Sample Output</b>    | <a href="#">show services rpm twamp server connection on page 669</a>                                                                                                                                                                                                                            |
| <b>Output Fields</b>            | <a href="#">Table 65 on page 657</a> lists the output fields for the <b>show services rpm twamp server connection</b> command. Output fields are listed in the approximate order in which they appear.                                                                                           |

**Table 69: show services rpm twamp server connection Output Fields**

| Field Name            | Field Description                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------|
| <b>Connection ID</b>  | Connection ID that uniquely identifies the connection between the TWAMP server and a particular client. |
| <b>Client address</b> | Client IP address.                                                                                      |
| <b>Client port</b>    | Client port number.                                                                                     |
| <b>Server address</b> | Server IP address.                                                                                      |
| <b>Server port</b>    | Server port number.                                                                                     |
| <b>Session count</b>  | Session count.                                                                                          |
| <b>Auth mode</b>      | Authentication mode.                                                                                    |

## Sample Output

### show services rpm twamp server connection

```

user@host> show services rpm twamp server connection
 Connection Client Client Server Server Session Auth
 ID address port address port count mode
 4 1.1.1.1 12345 192.168.219.203 890 16 none

```

|               |     |                 |       |           |       |    |      |
|---------------|-----|-----------------|-------|-----------|-------|----|------|
|               | 78  | 3.22.1.55       | 345   | 22.2.2.2  | 89022 | 5  | none |
|               | 234 | 192.168.219.203 | 2345  | 2.2.22.2  | 3333  | 16 | none |
|               | 5   | 221.4.1.1       | 82345 | 2.2.2.2   | 45909 | 16 |      |
| authenticated | 1   | 192.168.1.1     | 645   | 32.2.2.23 | 2394  | 16 |      |
| encrypted     |     |                 |       |           |       |    |      |



## show services rpm twamp server session

|                                 |                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show services rpm twamp server session</b><br><i>&lt;session-id&gt;</i>                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.3.                                                                                                                                                                                                                                                   |
| <b>Description</b>              | Display information about the sessions established between the real-time performance monitoring (RPM) Two-Way Active Measurement Protocol (TWAMP) server and control clients. By default, all established sessions are displayed, unless you specify a session ID when you issue the command. |
| <b>Options</b>                  | <i>session-id</i> —(Optional) Display only information about the specified session ID.                                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">show services rpm twamp server session on page 671</a>                                                                                                                                                                                                                            |
| <b>Output Fields</b>            | <a href="#">Table 70 on page 671</a> lists the output fields for the <b>show services rpm twamp server session</b> command. Output fields are listed in the approximate order in which they appear.                                                                                           |

**Table 70: show services rpm twamp server session Output Fields**

| Field Name               | Field Description                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Session ID</b>        | Session ID that uniquely identifies the session between the TWAMP server and a particular client.       |
| <b>Connection ID</b>     | Connection ID that uniquely identifies the connection between the TWAMP server and a particular client. |
| <b>Sender address</b>    | Sender IP address.                                                                                      |
| <b>Sender port</b>       | Sender port number.                                                                                     |
| <b>Reflector address</b> | Reflector IP address.                                                                                   |
| <b>Reflector port</b>    | Reflector port number.                                                                                  |

## Sample Output

### show services rpm twamp server session

```

user@host> show services rpm twamp server session
 Session Connection Sender Sender Reflector Reflector
 ID ID address port address port

 4 44 1.1.1.1 12345 192.168.219.203 890
 78 44 3.22.1.55 345 22.2.2.2 89022
 234 423 192.168.219.203 2345 2.2.22.2 3333
 5 423 221.4.1.1 82345 2.2.2.2 45909
 1 423 192.168.1.1 645 32.2.2.23 2394

```



## show services service-sets statistics jflow-log

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services service-sets statistics jflow-log<br><interface <i>interface-name</i> ><br><service-set <i>service-set-name</i> ><br><brief   detail>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Command introduced in Junos OS Release 15.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Display statistical information on the logs or records generated in flow monitoring format with optional filtering by interface and service set name..                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>none</b>—Display the statistical details on flow monitoring logs for NAT events for all services interfaces and all service sets.</p> <p><b>brief</b>—(Default) Display abbreviated flow monitoring log statistics.</p> <p><b>detail</b>—Display detailed flow monitoring log statistics.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Display the flow monitoring log statistics for a specific adaptive service interface. On M Series and T Series routers, <i>interface-name</i> can be <i>ms-fpc/pic/port</i>. It is supported only on MS-MICs and MS-MPCs.</p> <p><b>service-set <i>service-set name</i></b>—(Optional) Display the flow monitoring log statistics for a specific named service-set.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">clear services service-sets statistics syslog</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>List of Sample Output</b>    | <a href="#">show services service-sets statistics jflow-log brief on page 676</a><br><a href="#">show services service-sets statistics jflow-log detail on page 676</a><br><a href="#">show services service-sets statistics jflow-log service-set on page 678</a><br><a href="#">show services service-sets statistics jflow-log service-set detail on page 678</a>                                                                                                                                                                                                                                                                                                                                                             |
| <b>Output Fields</b>            | <a href="#">Table 71 on page 673</a> lists the output fields for the <b>show services service-sets statistics jflow-log</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Table 71: show services service-sets statistics jflow-log Output Fields**

| Field Name       | Field Description                                                                                | Level of Output |
|------------------|--------------------------------------------------------------------------------------------------|-----------------|
| Interface        | Name of a services interface.                                                                    | all             |
| Rate limit       | Maximum number of NAT error events for which records in flow monitoring format must be recorded. | all             |
| Template records | Details of the template records in flow monitoring log messages.                                 | all             |
| Sent             | Number of template records sent to a collector                                                   | all             |

Table 71: show services service-sets statistics jflow-log Output Fields (*continued*)

| Field Name                     | Field Description                                                                           | Level of Output |
|--------------------------------|---------------------------------------------------------------------------------------------|-----------------|
| <b>Messages dropped</b>        | Number of template records dropped while transmission to a collector.                       | all             |
| <b>Data records</b>            | Details of the data records in flow monitoring log messages.                                | all             |
| <b>Sent</b>                    | Number of data records sent to a collector.                                                 | all             |
| <b>Dropped</b>                 | Number of data records dropped while transmission to a collector                            | all             |
| <b>Service set</b>             | Name of a service set.                                                                      | all             |
| <b>Unresolvable collectors</b> | Number of collectors that cannot be traced and be reached to export records for NAT events. | all             |

Table 71: show services service-sets statistics jflow-log Output Fields (*continued*)

| Field Name        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Level of Output |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>class name</b> | <p>Logs created for events for each of the following classes:</p> <ul style="list-style-type: none"> <li>• <b>NAT44 Session logs</b>—Details of logs created for NAT44 sessions</li> <li>• <b>NAT64 Session logs</b>—Details of logs created for NAT64 sessions</li> <li>• <b>NAT44 BIB logs</b>—Details of logs created for NAT44 binding information bases, which is a table of bindings kept by a NAT44. Each NAT44 has a BIB for each translated protocol.</li> <li>• <b>NAT64 BIB logs</b>—Details of logs created for NAT44 binding information bases, which is a table of bindings kept by a NAT64. Each NAT64 has a BIB for each translated protocol.</li> <li>• <b>NAT Address Exhausted logs</b>—Details of logs created for exhaustion of NAT addresses</li> <li>• <b>NAT Port Exhausted logs</b>—Details of logs created for exhaustion of NAT pool</li> <li>• <b>NAT44 Quota Exceeded logs</b>—Details of logs created when allocated quota is exceeded for NAT44 events</li> <li>• <b>NAT64 Quota Exceeded logs</b>—Details of logs created when allocated quota is exceeded for NAT64 events</li> <li>• <b>NAT44 Address Bind logs</b>—Details of logs generated for address bindings for NAT44 events</li> <li>• <b>NAT64 Address Bind logs</b>—Details of logs generated for address bindings for NAT64 events</li> <li>• <b>NAT44 PBA logs</b>—Details of logs generated for NAT44 port block allocation events</li> <li>• <b>NAT64 PBA logs</b>—Details of logs generated for NAT64 port block allocation events</li> </ul> <p>The following information is displayed for flow monitoring log messages for each class of event that is logged:</p> <ul style="list-style-type: none"> <li>• <b>Template records</b>—Details of the template records in flow monitoring log messages</li> <li>• <b>Sent</b>—Number of template records sent to a collector</li> <li>• <b>Dropped</b>—Number of template records dropped while transmission to a collector</li> <li>• <b>Data records</b>—Details of the data records in flow monitoring log messages</li> <li>• <b>Sent</b>—Number of data records sent to a collector</li> <li>• <b>Dropped</b>—Number of data records dropped while transmission to a collector. Counts are provided for the drop reasons</li> <li>• <b>socket send error</b>—Number of times a socket was not opened for data transmission</li> <li>• <b>no memory</b>—Number of messages dropped because of insufficient memory</li> <li>• <b>invalid data</b>—Number of messages dropped because of invalid data in the records</li> <li>• <b>above rate limit</b>—The maximum number of flow monitoring log messages per second was exceeded.</li> </ul> | <b>detail</b>   |

## Sample Output

### show services service-sets statistics jflow-log brief

```
user@host> show services service-sets statistics jflow-log brief
Interface: ms-5/0/0
Rate limit: 1000
Template records:
 Sent: 36
 Dropped: 0
Data records:
 Sent: 2
 Dropped: 0

Service-set: sset_44
Unresolvable collectors: 0
Template records:
 Sent: 36
 Dropped: 0
Data records:
 Sent: 2
 Dropped: 0
```

## Sample Output

### show services service-sets statistics jflow-log detail

```
user@host> show services service-sets statistics jflow-log detail
Interface: ms-5/0/0
Rate limit: 1000
Template records:
 Sent: 48
 Dropped: 0
Data records:
 Sent: 4
 Dropped: 0

Service-set: sset_44
Unresolvable collectors: 0
Template records:
 Sent: 48
 Dropped: 0
Data records:
 Sent: 4
 Dropped: 0
NAT44 Session logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 4
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 Session logs:
 Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 BIB logs:
```

```
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 BIB logs:
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT Address Exhausted logs:
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT Port Exhausted logs:
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 Quota Exceeded logs:
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 Quota Exceeded logs:
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 Address Bind logs:
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 Address Bind logs:
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 PBA logs:
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
```

```
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 PBA logs:
Template records:
 Sent: 4
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
```

#### show services service-sets statistics jflow-log service-set

```
user@host> show services service-sets statistics jflow-log service-set sset_44
Interface: ms-5/0/0
```

```
Service-set: sset_44
Unresolvable collectors: 0
Template records:
 Sent: 72
 Dropped: 0
Data records:
 Sent: 4
 Dropped: 0
```

#### show services service-sets statistics jflow-log service-set detail

```
user@host> show services service-sets statistics jflow-log service-set sset_44 detail
Interface: ms-5/0/0
```

```
Service-set: sset_44
Unresolvable collectors: 0
Template records:
 Sent: 84
 Dropped: 0
Data records:
 Sent: 4
 Dropped: 0
NAT44 Session logs:
Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 4
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 Session logs:
Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 BIB logs:
Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 BIB logs:
Template records:
 Sent: 7
```



```

 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT Address Exhausted logs:
 Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT Port Exhausted logs:
 Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 Quota Exceeded logs:
 Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 Quota Exceeded logs:
 Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 Address Bind logs:
 Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 Address Bind logs:
 Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT44 PBA logs:
 Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)
NAT64 PBA logs:
 Template records:
 Sent: 7
 Dropped: 0 (socket send error: 0, no memory: 0)
 Data records:
 Sent: 0
 Dropped: 0 (invalid data: 0, no memory: 0, above rate limit: 0)

```



## show services video-monitoring mdi errors fpc-slot

|                                 |                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services video-monitoring mdi errors fpc-slot <i>fpc-slot</i>                                                                                                                              |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1.                                                                                                                                                    |
| <b>Description</b>              | Display video monitoring error statistics.                                                                                                                                                      |
| <b>Options</b>                  | <i>fpc-slot</i> —Number of the fpc slot for which statistics are displayed.                                                                                                                     |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Inline Video Monitoring Overview on page 309</a></li> </ul>                                                                                |
| <b>List of Sample Output</b>    | <a href="#">show services video-monitoring mdi errors fpc-slot on page 681</a>                                                                                                                  |
| <b>Output Fields</b>            | Table 33 on page 316 lists the output fields for the <b>show services video-monitoring mdi errors fpc-slot</b> command. Output fields are listed in the approximate order in which they appear. |

Table 72: show services video-monitoring mdi errors fpc-slot Output Fields

| Field Name                      | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FPC slot                        | Slot number of the monitored FPC.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Flow Insert Error               | Number of errors during new flow insert operations.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Flow Policer Drops              | <p>Number of packets dropped by flow policer process.</p> <p><b>NOTE:</b> New flows usually arrive within a very short time interval (1.5 microseconds). These errors do not represent the loss of entire flows, because subsequent packets in the flow can establish the flow. All packets are monitored after a flow has been established. Packet forwarding occurs independently of the video monitoring, and packets are not dropped due to video monitoring errors.</p> |
| Unsupported Media Packets Count | Number of packets dropped because they are not media packets or they are unsupported media packets.                                                                                                                                                                                                                                                                                                                                                                          |
| PID Limit Exceeded              | <p>Number of packets unmonitored because the process identifier (PID) limit exceeded has been exceeded.</p> <p><b>NOTE:</b> The current PID limit is 6.</p>                                                                                                                                                                                                                                                                                                                  |

## Sample Output

### show services video-monitoring mdi errors fpc-slot

```
user@host> show services video-monitoring mdi errors fpc-slot 2
```

MDI Errors Information

FPC Slot: 2

Flow Insert Error: 0, Flow Policer Drops: 0

Unsupported Media Packets Count: 0, PID Limit Exceeded: 202995

## show services video-monitoring mdi flows fpc-slot

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show services video-monitoring mdi flows fpc-slot <i>fpc-slot</i> &lt;brief&gt; &lt;count&gt; &lt;destination-address&gt; &lt;destination-port&gt; &lt;detail&gt; &lt;input&gt; &lt;interface-name&gt; &lt;output&gt; &lt;rtp&gt; &lt;source-address&gt; &lt;source-port&gt; &lt;template-name&gt; &lt;udp&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Display inline video monitoring flow statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b>fpc-slot</b>—Number of the slot for which flows are reported.</p> <p><b>brief</b>—(Optional) Display brief output(default).</p> <p><b>count</b>—(Optional) Display the number of flows.</p> <p><b>destination-address</b>—(Optional) Filter output by destination address.</p> <p><b>destination-port</b>—(Optional) Filter output by destination port.</p> <p><b>detail</b>—(Optional) Display output in detailed format including media delivery index records.</p> <p><b>input</b>—(Optional) Filter output by flow direction input.</p> <p><b>interface-name</b>—(Optional) Filter output by logical interface name.</p> <p><b>output</b>—(Optional) Filter output by flow direction output.</p> <p><b>rtp</b>—(Optional) Filter output by flow type rtp.</p> <p><b>source-address</b>—(Optional) Filter output by source IP address.</p> <p><b>source-port</b>—(Optional) Filter output by source port.</p> <p><b>template-name</b>—(Optional) Filter output by media delivery index template name.</p> <p><b>udp</b>—(Optional) Filter output by flow type MPEG-TS.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Related Documentation

- [Inline Video Monitoring Overview on page 309](#)

## List of Sample Output

[show services video-monitoring mdi flows fpc-slot brief on page 684](#)  
[show services video-monitoring mdi flows fpc-slot detail on page 685](#)

## Output Fields

[Table 34 on page 316](#) lists the output fields for the **show services video-monitoring mdi flows fpc-slot** command. Output fields are listed in the approximate order in which they appear.

**Table 73: show services mdi flows Output Fields**

| Field Name    | Field Description                                                          |
|---------------|----------------------------------------------------------------------------|
| SIP           | Source IP address                                                          |
| DIP           | Destination IP address                                                     |
| SP            | Source port                                                                |
| DP            | Destination port                                                           |
| Di            | Direction (I=Input, O=Output)                                              |
| Ty            | Type of flow                                                               |
| Last DF:MLR   | Delay factor and media loss rate value of last media delivery index record |
| Avg DF:MLR    | Average value of delay factor and media loss rate                          |
| Last MRV      | Media rate variation value of last media delivery index record             |
| Avg MRV       | Average value of media rate variation                                      |
| IFL           | Interface name on which flow is receiving                                  |
| Template Name | Name of template associated with flow                                      |

## Sample Output

**show services video-monitoring mdi flows fpc-slot brief**

```
user@host> show services video-monitoring mdi flows fpc-slot 2 brief
```

| Sno        | SIP      | SP      | DIP      | DP            | Di         | Ty  | Last DF:MLR | Avg |
|------------|----------|---------|----------|---------------|------------|-----|-------------|-----|
| DF:MLR     | Last MRV | Avg MRV | IFL      | Template Name |            |     |             |     |
| 1          | 20.0.0.2 | 1024    | 30.0.0.2 | 2048          | I          | UDP | 70.90:1     |     |
| 92.15:8205 | -7.09    | -9.36   |          |               | xe-2/2/1.0 |     | t1          |     |

## Sample Output

### show services video-monitoring mdi flows fpc-slot detail

```
user@host> show services video-monitoring flows fpc-slot 2 detail count 19
```

Format for RTP flows:

```
Source Address: 20.0.0.2, Source Port: 1024
Destination Address: 30.0.0.2, Destination Port: 2048
Last DF:MLR: 3.58:0, Avg DF:MLR: 3.60:0
Last MRV: 0.00, Avg MRV: 0.00
Interface Name: xe-2/2/1.0, Template Name: t1
Flow Direction: Input, Flow Type: RTP, MDI Records Count: 10
```

| Rec No | DF   | MLR | MRV  |
|--------|------|-----|------|
| 1      | 3.58 | 0   | 0.00 |
| 2      | 3.62 | 0   | 0.00 |
| 3      | 3.59 | 0   | 0.00 |
| 4      | 3.63 | 0   | 0.00 |
| 5      | 3.60 | 0   | 0.00 |
| 6      | 3.64 | 0   | 0.00 |
| 7      | 3.61 | 0   | 0.00 |
| 8      | 3.57 | 0   | 0.00 |
| 9      | 3.62 | 0   | 0.00 |
| 10     | 3.58 | 0   | 0.00 |

Format for MPEG2-TS over UDP flows:

```
Source Address: 20.0.0.2, Source Port: 1024
Destination Address: 30.0.0.2, Destination Port: 2048
Last DF:MLR: 3.63:0, Avg DF:MLR: 3.61:4097
Last MRV: 0.00, Avg MRV: 0.00
Interface Name: xe-2/2/1.0, Template Name: t1
Flow Direction: Input, Flow Type: UDP, MDI Records Count: 10
```

| Rec No | DF     | MLR   | MRV  | PID-0  | PID-1  | PID-2  |
|--------|--------|-------|------|--------|--------|--------|
|        | PID-3  | PID-4 |      | PID-5  |        |        |
| MLR    | Val    | MLR   | Val  | MLR    | Val    | MLR    |
| 1      | 3.63   | 0     | 0.00 | 0x1f40 | 0      | 0x1f41 |
| 0      | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |
| 2      | 3.59   | 0     | 0.00 | 0x1f40 | 0      | 0x1f41 |
| 0      | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |
| 3      | 3.64   | 0     | 0.00 | 0x1f40 | 0      | 0x1f41 |
| 0      | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |
| 4      | 3.60   | 0     | 0.00 | 0x1f40 | 0      | 0x1f41 |
| 0      | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |
| 5      | 3.64   | 0     | 0.00 | 0x1f40 | 0      | 0x1f41 |
| 0      | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |
| 6      | 3.61   | 0     | 0.00 | 0x1f40 | 0      | 0x1f41 |
| 0      | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |
| 7      | 3.57   | 0     | 0.00 | 0x1f40 | 0      | 0x1f41 |
| 0      | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |
| 8      | 3.62   | 0     | 0.00 | 0x1f40 | 0      | 0x1f41 |
| 0      | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |

|    |        |       |      |        |        |        |        |      |
|----|--------|-------|------|--------|--------|--------|--------|------|
| 9  | 3.58   | 40977 | 0.00 | 0x1f40 | 40977  | 0x1f41 | 0      | 0x12 |
| 0  | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |        |      |
| 10 | 3.63   | 0     | 0    | 0.00   | 0x1f40 | 0      | 0x1f41 | 0    |
| 0  | 0x1f54 | 0     | 0x11 | 0      | 0x1020 | 0      |        |      |



## show services video-monitoring mdi stats fpc-slot

|                                 |                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show services video-monitoring mdi stats fpc-slot <i>fpc-slot</i>                                                                                                                              |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1.                                                                                                                                                   |
| <b>Description</b>              | Display inline video monitoring statistics.                                                                                                                                                    |
| <b>Options</b>                  | <i>fpc-slot</i> —Number of the fpc slot for which statistics are displayed.                                                                                                                    |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Inline Video Monitoring Overview on page 309</a></li> </ul>                                                                               |
| <b>List of Sample Output</b>    | <a href="#">show services video-monitoring mdi stats fpc-slot on page 688</a>                                                                                                                  |
| <b>Output Fields</b>            | Table 32 on page 315 lists the output fields for the <b>show services video-monitoring mdi stats fpc-slot</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 74: show services video-monitoring mdi stats fpc-slot Output Fields**

| Field Name           | Field Description                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FPC Slot             | Slot number of the monitored FPC                                                                                                                                                 |
| Active Flows         | Number of active flows currently monitored.<br>active flows = inserted flows - deleted flows.                                                                                    |
| Total Inserted Flows | Number of flows initiated under video monitoring.                                                                                                                                |
| Total Deleted Flows  | Number of flows deleted due to inactivity timeout.                                                                                                                               |
| Total Packets Count  | Number of total packets monitored.                                                                                                                                               |
| Total Bytes Count    | Number of total bytes monitored.                                                                                                                                                 |
| DF Alarm Count       | Number of delay factor alarms at each of the following levels: <ul style="list-style-type: none"> <li>• Info level</li> <li>• Warning level</li> <li>• Critical level</li> </ul> |

**Table 74: show services video-monitoring mdi stats fpc-slot Output Fields (*continued*)**

| Field Name             | Field Description                                                                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MLR Alarm Count</b> | Number of media loss rate (MLR) alarms at each of the following levels: <ul style="list-style-type: none"><li>• Info level</li><li>• Warning level</li><li>• Critical level</li></ul>      |
| <b>MRV alarm count</b> | Number of media rate variation (MRV) alarms at each of the following levels: <ul style="list-style-type: none"><li>• Info level</li><li>• Warning level</li><li>• Critical level</li></ul> |

## Sample Output

### show services video-monitoring mdi stats fpc-slot

```
user@host> show services video-monitoring mdi stats fpc-slot 2
MDI Stats Information
FPC Slot: 2
Active Flows: 1, Total Inserted Flows: 1, Total Deleted Flows: 0
Total Packets Count: 746284, Total Bytes Count: 1013453672
DF alarm count: 0, Info level: 0, Warning level: 0, Critical level: 0
MLR alarm count: 0, Info level: 0, Warning level: 0, Critical level: 0
MRV alarm count: 0, Info level: 0, Warning level: 0, Critical level: 0
```

## test services rpm rfc2544-benchmarking test

**Syntax** test services rpm rfc2544-benchmarking test(ACX Series)  
 <clear-counters>  
 <routing-instance>  
 <test-name>  
 <test-id>  
 <start>>  
 <stop>

**Syntax** test services rpm rfc2544-benchmarking test(MX104 Router)  
 <test-name>  
 <test-id>  
 <start>>  
 <stop>

**Release Information** Command introduced in Junos OS Release 12.3X52 for ACX Series routers.  
 Command introduced in Junos OS Release 13.3R1 for MX104 3D Universal Edge Routers.

**Description** Start or stop an RFC 2544-based benchmarking test. You can start or stop all of the test names that are defined on a router, or start or stop a specific test name. You can also stop a test based on its test identifier. You can also clear the statistical counters associated with the test. When you trigger an RFC 2544-based benchmarking test, it passes through a series of states. These states are displayed in the Test state field in the brief or displayed output information of the **show services rpm rfc2544-benchmarking** command.



**NOTE:** The RFC 2544 test is stopped at the initiator automatically after the test successfully completes all of the test steps. You need not explicitly enter the **test services rpm rfc2544-benchmarking test <test-name | test-id> stop** command. However, at the reflector, you must explicitly enter this command to stop the test after the test is completed at the initiator.

**Options** **start**—Start the RFC 2544-based benchmarking test

**stop**—Terminate the RFC 2544-based benchmarking test

**clear-counters**—(ACX Series routers only) Clear the statistics associated with the benchmarking test that was run.

**routing-instance**—(ACX Series routers only) Name of the routing instance for the test.

**test-name**—Name of the benchmarking test that must be started or stopped.

**test-id**—Unique identifier of the test that must be stopped. You can stop a test based on the test identifier. You can use the **test-id** option with only the **test services rpm rfc2544-benchmarking stop** command.

**Additional Information** The test session is supported in out-of-service mode for the underlying service. You must not transmit any traffic to the UNI port, configured as a generator or a reflector, that is being tested during the duration of the test.

**Required Privilege Level** view

**Related Documentation**

- [Configuring an RFC 2544-Based Benchmarking Test on page 235](#)
- [RFC2544-Based Benchmarking Tests Overview on page 227](#)
- [rfc2544-benchmarking on page 477](#)

**List of Sample Output** [test services rpm rfc2544-benchmarking test start on page 690](#)

**Output Fields** To display the results of the benchmarking test, use the **show services rpm rfc2544-benchmarking test start** command.

## Sample Output

**test services rpm rfc2544-benchmarking test start**

```
user@host> test services rpm rfc2544-benchmarking test test1 start
Test "test1" id 56 started
```

The response specifies that a test has been started with test id 56. The test ID can be further used in **show** commands to view test output.

## PART 6

# Index

- [Index on page 693](#)



# Index

## Symbols

|                                              |      |
|----------------------------------------------|------|
| #, comments in configuration statements..... | xxiv |
| ( ), in syntax descriptions.....             | xxiv |
| < >, in syntax descriptions.....             | xxiv |
| [ ], in configuration statements.....        | xxiv |
| { }, in configuration statements.....        | xxiv |
| (pipe), in syntax descriptions.....          | xxiv |

## A

|                                              |                                        |
|----------------------------------------------|----------------------------------------|
| accept                                       |                                        |
| action.....                                  | 104                                    |
| accounting statement                         |                                        |
| flow monitoring.....                         | 338                                    |
| usage guidelines.....                        | 115                                    |
| active flow monitoring                       |                                        |
| aggregated flows, displaying.....            | 579                                    |
| available PICs, displaying.....              | 602                                    |
| CPU usage, displaying.....                   | 605                                    |
| error statistics, displaying.....            | 584                                    |
| flow statistics, displaying.....             | 588                                    |
| flows, detailed information, displaying..... | 593                                    |
| memory statistics, displaying.....           | 598                                    |
| packet size distribution, displaying.....    | 600                                    |
| adaptive-services-pics statement             |                                        |
| usage guidelines.....                        | 46                                     |
| address statement                            |                                        |
| DFC.....                                     | 339                                    |
| usage guidelines.....                        | 82                                     |
| flow monitoring.....                         | 339                                    |
| usage guidelines.....                        | 104                                    |
| aggregate-export-interval statement.....     | 340                                    |
| usage guidelines.....                        | 115                                    |
| aggregated flows, displaying.....            | 579                                    |
| aggregation statement                        |                                        |
| flow monitoring.....                         | 341                                    |
| usage guidelines.....                        | 132                                    |
| alarms                                       |                                        |
| statement.....                               | 342, 343, 366, 405, 435, 436, 447, 501 |
| allowed-destinations statement.....          | 344                                    |
| usage guidelines.....                        | 83                                     |

|                                       |     |
|---------------------------------------|-----|
| analyzer-address statement.....       | 344 |
| usage guidelines.....                 | 37  |
| analyzer-id statement.....            | 345 |
| usage guidelines.....                 | 37  |
| archive-sites statement.....          | 345 |
| usage guidelines.....                 | 38  |
| AS PIC                                |     |
| redundancy.....                       | 21  |
| authentication-key-chain statement    |     |
| RPM.....                              | 347 |
| authentication-mode statement         |     |
| RPM.....                              | 346 |
| autonomous-system-type statement..... | 348 |
| usage guidelines.....                 | 132 |

## B

|                                            |      |
|--------------------------------------------|------|
| benchmarking test See RFC2544 benchmarking |      |
| test, RPM service                          |      |
| bgp statement                              |      |
| RPM.....                                   | 349  |
| braces, in configuration statements.....   | xxiv |
| brackets                                   |      |
| angle, in syntax descriptions.....         | xxiv |
| square, in configuration statements.....   | xxiv |

## C

|                                                   |     |
|---------------------------------------------------|-----|
| capture-group statement.....                      | 350 |
| usage guidelines.....                             | 81  |
| cflowd statement                                  |     |
| usage guidelines.....                             | 132 |
| clear passive-monitoring statistics command.....  | 537 |
| clear services accounting statistics inline-jflow |     |
| command.....                                      | 538 |
| clear services dynamic-flow-capture               |     |
| command.....                                      | 539 |
| clear services flow-collector statistics          |     |
| command.....                                      | 540 |
| clear services rpm twamp server connection        |     |
| command.....                                      | 541 |
| clear services service-sets statistics jflow-log  |     |
| command.....                                      | 542 |
| clear services video-monitoring mdi errors        |     |
| command.....                                      | 543 |
| clear services video-monitoring mdi statistics    |     |
| command.....                                      | 544 |
| client statement.....                             | 353 |
| client-list statement.....                        | 354 |
| collector statement.....                          | 354 |
| usage guidelines.....                             | 38  |

|                                                                          |        |
|--------------------------------------------------------------------------|--------|
| collector statement (flow monitoring logs for NAT events).....           | 355    |
| collector statement (flow template profiles for NAT events).....         | 356    |
| collector-group statement (flow monitoring logs for NAT events).....     | 358    |
| collector-group statement (flow template profiles for NAT events).....   | 357    |
| collector-pic statement                                                  |        |
| usage guidelines.....                                                    | 46     |
| comments, in configuration statements.....                               | xxiv   |
| configuration                                                            |        |
| dynamic flow capture interface.....                                      | 87     |
| flow collector interface.....                                            | 40     |
| flow-tap application.....                                                | 97     |
| content destination                                                      |        |
| dynamic flow capture, displaying.....                                    | 607    |
| content destinations                                                     |        |
| DFC.....                                                                 | 79     |
| Junos Packet Vision.....                                                 | 92     |
| content-destination statement.....                                       | 359    |
| usage guidelines.....                                                    | 82     |
| control source                                                           |        |
| DFC.....                                                                 | 79     |
| control source,                                                          |        |
| dynamic flow capture, displaying.....                                    | 609    |
| control-connection statement.....                                        | 360    |
| control-source statement.....                                            | 361    |
| usage guidelines.....                                                    | 83     |
| conventions                                                              |        |
| text and syntax.....                                                     | xxiii  |
| core-dump statement.....                                                 | 362    |
| usage guidelines.....                                                    | 6      |
| curly braces, in configuration statements.....                           | xxiv   |
| customer support.....                                                    | xxv    |
| contacting JTAC.....                                                     | xxv    |
| <b>D</b>                                                                 |        |
| data-fill statement.....                                                 | 363    |
| data-fill-with-zeros statement.....                                      | 364    |
| data-format statement.....                                               | 364    |
| usage guidelines.....                                                    | 37     |
| data-size statement.....                                                 | 365    |
| destination statement.....                                               | 367    |
| flow monitoring                                                          |        |
| usage guidelines.....                                                    | 104    |
| destination-address statement (flow monitoring logs for NAT events)..... | 368    |
| destination-interface statement                                          |        |
| RPM.....                                                                 | 369    |
| destination-ipv4-address (RFC 2544 Benchmarking).....                    | 370    |
| destination-mac-address (RFC2544 Benchmarking).....                      | 371    |
| destination-port statement                                               |        |
| RPM.....                                                                 | 372    |
| destination-port statement (flow monitoring logs for NAT events).....    | 373    |
| destination-udp-port (RFC 2544 Benchmarking).....                        | 373    |
| destinations statement                                                   |        |
| flow collection.....                                                     | 374    |
| usage guidelines.....                                                    | 36     |
| DFC                                                                      |        |
| architecture.....                                                        | 79     |
| capture group.....                                                       | 81     |
| control source configuration.....                                        | 83     |
| destination configuration.....                                           | 82     |
| example configuration.....                                               | 87     |
| interface configuration.....                                             | 84     |
| system logging.....                                                      | 85     |
| threshold configuration.....                                             | 86     |
| direction (RFC2544 Benchmarking).....                                    | 375    |
| disable statement                                                        |        |
| flow monitoring.....                                                     | 376    |
| traffic sampling                                                         |        |
| usage guidelines.....                                                    | 107    |
| disable-signature-check (RFC 2544 Benchmarking).....                     | 377    |
| discard accounting                                                       |        |
| usage guidelines.....                                                    | 115    |
| documentation                                                            |        |
| comments on.....                                                         | xxv    |
| dscp-code-point statement                                                |        |
| RPM.....                                                                 | 378    |
| DTCP.....                                                                | 79, 91 |
| duplicates-dropped-periodicity statement.....                            | 379    |
| usage guidelines.....                                                    | 87     |
| dynamic flow capture See DFC                                             |        |
| content destination, displaying.....                                     | 607    |
| control source, displaying.....                                          | 609    |
| statistics                                                               |        |
| clearing.....                                                            | 539    |
| displaying.....                                                          | 611    |
| dynamic flow capture interfaces                                          |        |
| displaying.....                                                          | 554    |
| Dynamic Tasking Control Protocol See DTCP                                |        |



dynamic-flow-capture statement.....380

## E

enable flow collection mode.....46

engine-id statement  
    flow monitoring.....381

engine-type statement.....382

export-format statement.....383  
    usage guidelines.....9

extension-service statement.....384

## F

family (RFC2544 Benchmarking).....388

family statement  
    flow monitoring  
        usage guidelines.....104

file statement.....391

    traffic sampling.....390

    traffic sampling output  
        usage guidelines.....108, 110

file-specification statement  
    usage guidelines.....37, 38

filename statement.....392

filename-prefix statement.....393  
    usage guidelines.....38

files  
    logging information output file.....110  
    traffic sampling output files.....108  
    var/log/sampled file.....110  
    var/tmp/sampled.pkts file.....108

files statement.....393  
    usage guidelines.....108

filter statement  
    flow monitoring.....394  
    usage guidelines.....104

firewall filters  
    actions.....104  
    in traffic sampling.....104

flow aggregation.....132  
    multiple flow servers.....167  
    source ID, IPFIX flows.....157  
    template and option template ID.....160  
    templates.....583  
    traffic sampling  
        observation domain ID, version 9 .....157

flow collector  
    analyzer configuration.....37  
    destination configuration.....36  
    example configuration.....40

file format configuration.....37

interface mapping.....38

transfer log.....38

flow collector interfaces  
    status information, displaying.....558

flow collector services  
    interface files, displaying.....614  
    packets received, displaying.....616  
    primary server, switching to.....545  
    secondary server, switching to.....546  
    statistics  
        displaying.....618  
        dropped-packet, clearing.....542  
        interface, clearing.....540  
    test file, transferring.....547

Flow monitoring  
    overview.....3, 25

flow monitoring  
    active  
        aggregated flows, displaying.....579  
        CPU usage, displaying.....605  
        detailed information, displaying.....593  
        error statistics, displaying.....584  
        flow statistics, displaying.....588  
        memory statistics, displaying.....598  
        packet size distribution, displaying.....600  
        PICs, displaying available.....602

    example configuration  
        multiple port mirroring.....182, 191  
        next-hop groups.....182, 191

    inline  
        flow statistics, clearing.....538

    passive  
        flow statistics, displaying.....571  
        memory and flow statistics,  
            displaying.....573  
        status, displaying.....575  
        usage statistics, displaying.....577  
    redundancy.....21

flow monitoring interfaces  
    status information, displaying.....564

flow server  
    replicating flows to multiple servers.....167

flow-active-timeout statement.....395  
    usage guidelines.....9

flow-collector statement.....396  
    usage guidelines.....35, 46

flow-export-destination statement.....397  
    usage guidelines.....9

|                                                 |        |                                                   |               |
|-------------------------------------------------|--------|---------------------------------------------------|---------------|
| flow-export-rate statement                      |        | inline-jflow statement                            |               |
| flow monitoring.....                            | 397    | flow monitoring.....                              | 410           |
| flow-inactive-timeout statement.....            | 398    | usage guidelines.....                             | 122, 125, 127 |
| usage guidelines.....                           | 9      | input-interface-index statement.....              | 411           |
| flow-monitoring statement.....                  | 399    | input-packet-rate-threshold statement.....        | 412           |
| flow-server statement                           |        | usage guidelines.....                             | 86            |
| flow monitoring.....                            | 400    | instance statement                                |               |
| flow-tap                                        |        | sampling.....                                     | 413           |
| interface.....                                  | 93     | usage guidelines.....                             | 114           |
| permissions statement.....                      | 94     | interface statement                               |               |
| RADIUS configuration.....                       | 94     | flow monitoring                                   |               |
| restrictions.....                               | 95     | usage guidelines.....                             | 176           |
| security.....                                   | 94     | flow-tap.....                                     | 415           |
| flow-tap application                            |        | usage guidelines.....                             | 93            |
| example configuration.....                      | 97     | interface-map statement.....                      | 416           |
| flow-tap statement.....                         | 402    | usage guidelines.....                             | 38            |
| flow-tap-dtcp statement.....                    | 94     | interfaces statement                              |               |
| font conventions.....                           | xxiii  | DFC.....                                          | 416           |
| forwarding-options statement                    |        | usage guidelines .....                            | 84            |
| usage guidelines.....                           | 328    | flow monitoring.....                              | 415           |
| ftp statement                                   |        | usage guidelines.....                             | 104           |
| usage guidelines.....                           | 36, 38 | video-monitoring.....                             | 417           |
| FTP traffic, sampling.....                      | 113    | IP addresses                                      |               |
|                                                 |        | sampling traffic from single IP addresses.....    | 112           |
| <b>G</b>                                        |        | ip-swap (RFC 2544 Benchmarking).....              | 418           |
| g-duplicates-dropped-periodicity statement..... | 404    | ipv4-template statement.....                      | 419           |
| usage guidelines.....                           | 87     | ipv6-template statement.....                      | 421           |
| g-max-duplicates statement.....                 | 405    |                                                   |               |
| usage guidelines.....                           | 87     | <b>J</b>                                          |               |
| <b>H</b>                                        |        | jflow-log (Services).....                         | 423           |
| hard-limit statement.....                       | 406    | jflow-log statement (flow monitoring logs for NAT |               |
| usage guidelines.....                           | 82     | events)                                           |               |
| hard-limit-target statement.....                | 406    | interfaces.....                                   | 422           |
| usage guidelines.....                           | 82     | Junos Packet Vision                               |               |
| hardware-timestamp statement.....               | 407    | application.....                                  | 91            |
| history-size statement.....                     | 407    | architecture.....                                 | 92            |
| usage guidelines.....                           | 212    |                                                   |               |
| host-outbound statement.....                    | 408    | <b>L</b>                                          |               |
| <b>I</b>                                        |        | label-position statement.....                     | 424           |
| in-service (RFC2544 Benchmarking).....          | 409    | lawful intercept architecture.....                | 92            |
| inactivity-timeout statement                    |        | license-server statement                          |               |
| RPM.....                                        | 409    | transmission of throughput data of services to    |               |
| inet6-options statement                         |        | a collector.....                                  | 425           |
| RPM.....                                        | 418    | local-dump statement.....                         | 426           |
| inline flow monitoring                          |        | usage guidelines.....                             | 170           |
| flow statistics, clearing.....                  | 538    | log output                                        |               |
|                                                 |        | traffic sampling.....                             | 110           |

- 
- logical-system statement
    - RPM.....426
    - usage guidelines.....212
  - M**
  - manuals
    - comments on.....xxv
  - match statement.....427
  - max-connection-duration statement.....427
  - max-duplicates statement.....428
    - usage guidelines.....87
  - max-packets-per-second statement.....429
    - usage guidelines.....105
  - maximum-age statement.....429
    - usage guidelines.....38
  - maximum-connections statement.....430
  - maximum-connections-per-client statement.....431
  - maximum-packet-length statement.....432
  - maximum-sessions statement.....433
  - maximum-sessions-per-connection
    - statement.....434
  - media delivery index
    - delay factor.....309
    - media loss rate.....309
    - media rate variation.....309
  - mediation devices
    - Junos Packet Vision.....92
  - minimum-priority statement.....438
    - usage guidelines.....83
  - mode (RFC 2544 Benchmarking).....438
  - monitoring statement.....439
    - usage guidelines.....8
  - moving-average-size statement.....440
  - MPLS
    - packets
      - passive flow monitoring.....28
  - mpls-ipv4-template statement.....440
  - mpls-template statement.....441
  - multiservice-options statement.....441
  - N**
  - name-format statement.....442
    - usage guidelines.....37
  - next-hop group for port mirroring.....190
  - next-hop groups.....173
  - next-hop statement.....443
    - next-hop groups
      - usage guidelines.....176
    - usage guidelines.....173
  - next-hop-group statement
    - forwarding-options.....444
    - port mirroring.....445
    - usage guidelines.....173, 176
  - no-core-dump statement.....362
    - usage guidelines.....6
  - no-filter-check statement.....445
    - usage guidelines.....173
  - no-local-dump statement.....426
    - usage guidelines.....170
  - no-remote-trace statement
    - flow monitoring.....446
  - no-stamp statement.....500
    - usage guidelines.....108
  - no-syslog statement
    - DFC.....446
    - flow monitoring.....501
    - usage guidelines.....85
  - no-world-readable statement
    - flow monitoring.....534
    - usage guidelines.....108
  - notification-targets statement.....447
    - usage guidelines.....83
  - O**
  - observation-domain-id statement.....448
  - offloading flows
    - configuring.....23
  - one-way-hardware-timestamp statement.....449
    - usage guidelines.....208
  - option-refresh-rate statement.....450
  - options-template-id statement.....451
  - output files
    - logging information output file.....110
    - traffic sampling output files.....108
  - output statement
    - discard accounting.....452
    - flow monitoring.....453
    - port mirroring.....454
    - sampling.....455
  - output-interface-index statement.....456
  - P**
  - packet size distribution, displaying.....600
  - parentheses, in syntax descriptions.....xxiv
  - passive flow monitoring.....3, 25
    - error statistics, displaying.....569
    - flow statistics, displaying.....571
    - memory statistics, displaying.....573

|                                           |          |                                                                                        |     |
|-------------------------------------------|----------|----------------------------------------------------------------------------------------|-----|
| MPLS packets.....                         | 28       | redundancy                                                                             |     |
| PICs, displaying available.....           | 575      | flow monitoring.....                                                                   | 21  |
| statistics, clearing.....                 | 537      | reflect-etype (RFC 2544 Benchmarking).....                                             | 474 |
| usage statistics, displaying.....         | 577      | reflect-mode (RFC2544 Benchmarking).....                                               | 473 |
| passive-monitor-mode statement.....       | 456      | refresh-rate statement (flow monitoring logs for<br>NAT events).....                   | 472 |
| usage guidelines.....                     | 26       | request services flow-collector change-destination<br>primary interface command.....   | 545 |
| password statement                        |          | request services flow-collector change-destination<br>secondary interface command..... | 546 |
| usage guidelines.....                     | 36, 38   | request services flow-collector test-file-transfer<br>command.....                     | 547 |
| peer-as-billing-template statement.....   | 458      | request services rpm twamp command.....                                                | 548 |
| pic-memory-threshold statement.....       | 458      | required-depth statement.....                                                          | 475 |
| usage guidelines.....                     | 86       | usage guidelines.....                                                                  | 29  |
| PICs                                      |          | retry statement.....                                                                   | 476 |
| active flow monitoring                    |          | usage guidelines.....                                                                  | 39  |
| available PICs, displaying.....           | 602      | retry-delay statement.....                                                             | 476 |
| CPU usage, displaying.....                | 605      | usage guidelines.....                                                                  | 39  |
| pop-all-labels statement.....             | 459      | RFC 2544 benchmarking test, RPM service                                                |     |
| usage guidelines.....                     | 29       | configuring.....                                                                       | 235 |
| port mirroring.....                       | 173      | example, configuring for Layer 3 IPv4<br>services.....                                 | 239 |
| disabling.....                            | 376      | example, configuring for NNI of Ethernet<br>pseudowires.....                           | 254 |
| displaying.....                           | 552      | example, configuring for UNI of Ethernet<br>pseudowires.....                           | 246 |
| port statement.....                       | 479      | layer 2 overview.....                                                                  | 231 |
| cflowd                                    |          | statistical details of a specific test ID,<br>displaying.....                          | 640 |
| usage guidelines.....                     | 132      | statistical details of a test type,<br>displaying.....                                 | 635 |
| flow monitoring.....                      | 460      | test name, configuring.....                                                            | 235 |
| RPM.....                                  | 460      | test profile, configuring.....                                                         | 235 |
| TWAMP.....                                | 461      | RFC2544 benchmarking test, RPM service                                                 |     |
| port-mirroring statement.....             | 462      | overview.....                                                                          | 227 |
| usage guidelines.....                     | 173      | route-record statement                                                                 |     |
| post-cli-implicit-firewall statement..... | 463      | usage guidelines.....                                                                  | 132 |
| pre-rewrite-tos statement.....            | 464      | routing-instance statement                                                             |     |
| usage guidelines.....                     | 107      | RPM.....                                                                               | 478 |
| probe statement                           |          | routing-instance-list statement                                                        |     |
| RPM.....                                  | 465      | TWAMP.....                                                                             | 480 |
| probe-count statement.....                | 466      | routing-instances statement                                                            |     |
| probe-interval statement.....             | 467      | RPM.....                                                                               | 481 |
| probe-limit statement.....                | 467      | usage guidelines.....                                                                  | 213 |
| probe-server statement.....               | 468      | RPM.....                                                                               | 199 |
| probe-type statement.....                 | 469      | example configuration.....                                                             | 217 |
| protocol                                  |          |                                                                                        |     |
| two-way active measurement.....           | 201      |                                                                                        |     |
| <b>R</b>                                  |          |                                                                                        |     |
| rate statement.....                       | 470      |                                                                                        |     |
| usage guidelines.....                     | 105, 173 |                                                                                        |     |
| receive-options-packets statement.....    | 471      |                                                                                        |     |
| usage guidelines.....                     | 26       |                                                                                        |     |
| receive-ttl-exceeded statement.....       | 471      |                                                                                        |     |
| usage guidelines.....                     | 26       |                                                                                        |     |

|                                                                                         |          |
|-----------------------------------------------------------------------------------------|----------|
| RPM services                                                                            |          |
| benchmark test, performing.....                                                         | 689      |
| benchmarking test                                                                       |          |
| configuring.....                                                                        | 235      |
| example, configuring for Layer 2 Reflection, ELAN, Bridge.....                          | 262      |
| example, configuring for Layer 3 IPv4 services.....                                     | 239      |
| example, configuring for NNI of Ethernet pseudowires.....                               | 254      |
| example, configuring for UNI of Ethernet pseudowires.....                               | 246      |
| example, configuring Layer 2 Reflection, ELAN, VPLS.....                                | 287      |
| layer 2 overview.....                                                                   | 231      |
| overview.....                                                                           | 227      |
| reflector commands.....                                                                 | 234      |
| benchmarking test results                                                               |          |
| displaying by test state.....                                                           | 635      |
| test ID, displaying.....                                                                | 640      |
| test type, displaying.....                                                              | 635      |
| displaying information of an RFC 2544 benchmarking test for a particular test type..... | 635      |
| displaying information of an RFC 2544 benchmarking test for a specific test ID.....     | 640      |
| probe results                                                                           |          |
| history, displaying.....                                                                | 625      |
| recent, displaying.....                                                                 | 628      |
| protocols and ports, displaying.....                                                    | 624      |
| rpm statement.....                                                                      | 482, 483 |
| RPM statements                                                                          |          |
| traceoptions.....                                                                       | 515      |
| RPM TWAMP client                                                                        |          |
| connections, displaying.....                                                            | 657      |
| sessions, displaying.....                                                               | 667      |
| sessions, starting and stopping.....                                                    | 548      |
| RPM TWAMP client services                                                               |          |
| probe results                                                                           |          |
| history, displaying.....                                                                | 659      |
| RPM TWAMP server                                                                        |          |
| connections, clearing.....                                                              | 541      |
| connections, displaying.....                                                            | 669      |
| sessions, displaying.....                                                               | 671      |
| RPM TWAMP services                                                                      |          |
| probe results                                                                           |          |
| recent, displaying.....                                                                 | 663      |
| run-length statement.....                                                               | 485      |
| usage guidelines.....                                                                   | 105, 173 |
| <b>S</b>                                                                                |          |
| sample (firewall filter action).....                                                    | 104      |
| sample-once statement                                                                   |          |
| flow monitoring.....                                                                    | 485      |
| usage guidelines.....                                                                   | 107      |
| sampled file.....                                                                       | 110      |
| sampled.pkts file.....                                                                  | 108      |
| sampling                                                                                |          |
| logical interface.....                                                                  | 105      |
| monitoring interface.....                                                               | 6        |
| next-hop-groups, displaying.....                                                        | 549      |
| port-mirroring instances, displaying.....                                               | 552      |
| sampling rate.....                                                                      | 105      |
| sampling statement.....                                                                 | 486, 488 |
| usage guidelines.....                                                                   | 104      |
| send cflowd records to flow collector.....                                              | 46       |
| server statement.....                                                                   | 489      |
| server-inactivity-timeout statement.....                                                | 489      |
| service-port statement.....                                                             | 490      |
| usage guidelines.....                                                                   | 83       |
| service-type (RFC2544 Benchmarking).....                                                | 490      |
| services sets                                                                           |          |
| jflow-log statistics                                                                    |          |
| clearing.....                                                                           | 542      |
| displaying.....                                                                         | 673      |
| services statement                                                                      |          |
| DFC                                                                                     |          |
| usage guidelines.....                                                                   | 81       |
| dynamic-flow-control                                                                    |          |
| usage guidelines.....                                                                   | 332      |
| flow control                                                                            |          |
| usage guidelines.....                                                                   | 333      |
| flow-monitoring.....                                                                    | 491      |
| flow-tap                                                                                |          |
| usage guidelines.....                                                                   | 335      |
| rpm                                                                                     |          |
| usage guidelines.....                                                                   | 335      |
| RPM.....                                                                                | 491      |
| services-options statement.....                                                         | 492      |
| shared-key statement.....                                                               | 493      |
| usage guidelines.....                                                                   | 83       |
| show forwarding-options next-hop-group                                                  |          |
| command.....                                                                            | 549      |
| show forwarding-options port-mirroring                                                  |          |
| command.....                                                                            | 552      |

|                                                   |     |                                                   |     |
|---------------------------------------------------|-----|---------------------------------------------------|-----|
| show interfaces (Dynamic Flow Capture)            |     | show services rpm twamp server connection         |     |
| command.....                                      | 554 | command.....                                      | 669 |
| show interfaces (Flow Collector) command.....     | 558 | show services rpm twamp server session            |     |
| show interfaces (Flow Monitoring) command.....    | 564 | command.....                                      | 671 |
| show passive-monitoring error command.....        | 569 | show services service-sets statistics jflow-log   |     |
| show passive-monitoring flow command.....         | 571 | command.....                                      | 673 |
| show passive-monitoring memory command.....       | 573 | show services video-monitoring mdi errors         |     |
| show passive-monitoring status command.....       | 575 | command.....                                      | 681 |
| show passive-monitoring usage command.....        | 577 | show services video-monitoring mdi flows          |     |
| show services accounting aggregation              |     | command.....                                      | 683 |
| command.....                                      | 579 | show services video-monitoring mdi stats          |     |
| show services accounting aggregation template     |     | command.....                                      | 687 |
| command.....                                      | 583 | size statement.....                               | 493 |
| show services accounting errors command.....      | 584 | usage guidelines.....                             | 110 |
| show services accounting flow command.....        | 588 | soft-limit statement.....                         | 494 |
| show services accounting flow-detail              |     | usage guidelines.....                             | 82  |
| command.....                                      | 593 | soft-limit-clear statement.....                   | 494 |
| show services accounting memory command.....      | 598 | usage guidelines.....                             | 82  |
| show services accounting packet-size-distribution |     | SONET interfaces                                  |     |
| command.....                                      | 600 | sampling SONET interfaces.....                    | 111 |
| show services accounting status command.....      | 602 | source-address statement                          |     |
| show services accounting usage command.....       | 605 | flow monitoring.....                              | 495 |
| show services dynamic-flow-capture                |     | usage guidelines.....                             | 8   |
| content-destination command.....                  | 607 | RPM.....                                          | 496 |
| show services dynamic-flow-capture control-source |     | source-addresses statement                        |     |
| command.....                                      | 609 | DFC.....                                          | 496 |
| show services dynamic-flow-capture statistics     |     | usage guidelines.....                             | 83  |
| command.....                                      | 611 | source-id statement.....                          | 497 |
| show services flow-collector file interface       |     | source-ip statement (flow monitoring logs for NAT |     |
| command.....                                      | 614 | events).....                                      | 498 |
| show services flow-collector input interface      |     | source-ipv4-address (RFC 2544                     |     |
| command.....                                      | 616 | Benchmarking).....                                | 499 |
| show services flow-collector interface            |     | source-mac-address (RFC2544                       |     |
| command.....                                      | 618 | Benchmarking).....                                | 499 |
| show services rpm active-servers command.....     | 624 | source-udp-port (RFC 2544 Benchmarking).....      | 500 |
| show services rpm history-results command.....    | 625 | stamp option.....                                 | 110 |
| show services rpm probe-results command.....      | 628 | stamp statement.....                              | 500 |
| show services rpm rfc2544-benchmarking            |     | usage guidelines.....                             | 108 |
| command.....                                      | 635 | statement                                         |     |
| show services rpm rfc2544-benchmarking test-id    |     | flow monitoring                                   |     |
| command.....                                      | 640 | usage guidelines.....                             | 110 |
| show services rpm twamp client connection         |     | services                                          |     |
| command.....                                      | 657 | usage guidelines.....                             | 46  |
| show services rpm twamp client history-results    |     | statistics                                        |     |
| command.....                                      | 659 | active flow error.....                            | 584 |
| show services rpm twamp client probe-results      |     | active flow instances.....                        | 588 |
| command.....                                      | 663 | active flow memory utilization.....               | 598 |
| show services rpm twamp client session            |     | aggregated active flow.....                       | 579 |
| command.....                                      | 667 |                                                   |     |

|                                                   |          |
|---------------------------------------------------|----------|
| clearing inline flow instances.....               | 538      |
| dynamic flow capture                              |          |
| clearing.....                                     | 539      |
| displaying.....                                   | 611      |
| support, technical See technical support          |          |
| syntax conventions.....                           | xxiii    |
| syslog statement                                  |          |
| flow monitoring.....                              | 501      |
| <b>T</b>                                          |          |
| target statement.....                             | 502      |
| RPM.....                                          | 502      |
| tcp statement                                     |          |
| RPM.....                                          | 503      |
| tcp-tickles statement.....                        | 526      |
| technical support                                 |          |
| contacting JTAC.....                              | xxv      |
| template-id statement.....                        | 522      |
| template-profile statement (flow monitoring logs  |          |
| for NAT events).....                              | 523      |
| template-refresh-rate statement.....              | 524      |
| template-type statement (flow monitoring logs for |          |
| NAT events).....                                  | 525      |
| templates                                         |          |
| flow aggregation.....                             | 583      |
| templates statement                               |          |
| video-monitoring.....                             | 504      |
| test services rpm rfc2544-benchmarking            |          |
| command.....                                      | 689      |
| test statement                                    |          |
| RPM.....                                          | 506      |
| test-interface (RFC 2544 Benchmarking)            |          |
| RPM.....                                          | 508      |
| test-interval statement.....                      | 509      |
| test-name (RFC 2544 Benchmarking).....            | 510      |
| test-session statement.....                       | 511      |
| tests (RFC 2544 Benchmarking).....                | 507      |
| thresholds statement                              |          |
| RPM.....                                          | 512      |
| timestamp option.....                             | 110      |
| traceoptions statement                            |          |
| flow monitoring.....                              | 514      |
| RPM.....                                          | 515      |
| tracing operations                                |          |
| RPM.....                                          | 215      |
| traffic sampling                                  |          |
| configuring.....                                  | 104      |
| disabling.....                                    | 107, 376 |
| example configurations.....                       | 111      |
| flow aggregation.....                             | 132      |
| default values, option template ID.....           | 160      |
| default values, template ID.....                  | 160      |
| observation domain ID, version 9 .....            | 157      |
| option template ID, version 9 and                 |          |
| IPFIX.....                                        | 160      |
| source ID, IPFIX.....                             | 157      |
| template ID, version 9 and IPFIX.....             | 160      |
| FTP traffic.....                                  | 113      |
| logging information output file.....              | 110      |
| output files.....                                 | 108      |
| SONET interfaces.....                             | 111      |
| traffic from single IP addresses.....             | 112      |
| transfer statement.....                           | 516      |
| usage guidelines.....                             | 37       |
| transfer-log-archive statement.....               | 517      |
| usage guidelines.....                             | 38       |
| traps statement.....                              | 518      |
| ttl statement                                     |          |
| DFC.....                                          | 519      |
| usage guidelines.....                             | 82       |
| TWAMP client                                      |          |
| connections, displaying.....                      | 657      |
| sessions, displaying.....                         | 667      |
| sessions, starting and stopping.....              | 548      |
| TWAMP server                                      |          |
| connections, clearing.....                        | 541      |
| connections, displaying.....                      | 669      |
| sessions, displaying.....                         | 671      |
| twamp statement.....                              | 520      |
| twamp-server statement.....                       | 521      |
| <b>U</b>                                          |          |
| udp statement                                     |          |
| RPM.....                                          | 526      |
| udp-tcp-port-swap (RFC 2544                       |          |
| Benchmarking).....                                | 527      |
| unit statement                                    |          |
| flow monitoring.....                              | 528      |
| usage guidelines.....                             | 104      |
| username statement                                |          |
| flow collection.....                              | 529      |
| usage guidelines.....                             | 38       |
| <b>V</b>                                          |          |
| var/log/sampled file.....                         | 110      |
| var/tmp/sampled.pkts file.....                    | 108      |
| variant statement.....                            | 529      |
| usage guidelines.....                             | 37       |

|                                                              |               |
|--------------------------------------------------------------|---------------|
| version statement                                            |               |
| flow monitoring.....                                         | 530           |
| usage guidelines.....                                        | 132           |
| version statement (flow monitoring logs for NAT events)..... | 531           |
| version-ipfix statement                                      |               |
| usage guidelines.....                                        | 122, 125, 127 |
| video monitoring                                             |               |
| alarms, MDI metrics.....                                     | 314           |
| configuring.....                                             | 311           |
| interface flow criteria.....                                 | 313           |
| media delivery indexing.....                                 | 312           |
| errors                                                       |               |
| clearing.....                                                | 543           |
| displaying.....                                              | 681           |
| flows                                                        |               |
| displaying.....                                              | 683           |
| information logged in                                        |               |
| SNMP traps, alarms.....                                      | 317           |
| media delivery index See media delivery index                |               |
| media delivery indexing                                      |               |
| SNMP Get requests.....                                       | 318           |
| syslog messages.....                                         | 314           |
| overview.....                                                | 309           |
| platform support.....                                        | 309           |
| SNMP traps.....                                              | 314           |
| statistics                                                   |               |
| clearing.....                                                | 544           |
| displaying.....                                              | 687           |
| video-monitoring statement                                   |               |
| video-monitoring.....                                        | 533           |

## W

|                          |     |
|--------------------------|-----|
| world-readable statement |     |
| flow monitoring.....     | 534 |
| usage guidelines.....    | 108 |