




Junos[®] OS

Security Services Administration Guide



Modified: 2019-06-21



Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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 Security Services Administration Guide
Copyright © 2019 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 <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xxxv
	Documentation and Release Notes	xxxv
	Using the Examples in This Manual	xxxv
	Merging a Full Example	xxxvi
	Merging a Snippet	xxxvi
	Documentation Conventions	xxxvii
	Documentation Feedback	xxxix
	Requesting Technical Support	xxxix
	Self-Help Online Tools and Resources	xl
	Creating a Service Request with JTAC	xl
Part 1	Port Security	
Chapter 1	Port Security Overview	3
	Overview of Port Security	3
	Port Security Features	3
	Understanding How to Protect Access Ports from Common Attacks	6
	Mitigation of Ethernet Switching Table Overflow Attacks	7
	Mitigation of Rogue DHCP Server Attacks	7
	Protection Against ARP Spoofing Attacks (Does not apply to QFX10000 Series Switches)	8
	Protection Against DHCP Snooping Database Alteration Attacks (Does not apply to QFX10000 Series Switches)	8
	Protection Against DHCP Starvation Attacks	8
	Configuring Port Security (ELS)	9
	Configuring Port Security (non-ELS)	11
	Enabling DHCP Snooping	12
	Enabling Dynamic ARP Inspection (DAI)	13
	Enabling IPv6 Neighbor Discovery Inspection	13
	Limiting Dynamic MAC Addresses on an Interface	13
	Enabling Persistent MAC Learning on an Interface	14
	Limiting MAC Address Movement	14
	Restricting a VoIP Client MAC Address in a VoIP VLAN	14
	Configuring Trusted DHCP Servers on an Interface	14
	Example: Configuring Port Security (non-ELS)	15

Part 2	IPSec	
Chapter 2	Understanding IPsec and Security Associations	25
	IPSec Terms and Acronyms	25
	Security Associations Overview	27
	IKE Key Management Protocol Overview	28
	IPsec Requirements for Junos-FIPS	30
Chapter 3	IPsec Configurations and Examples	31
	Considering General IPsec Issues	31
	IPsec Configuration for an ES PIC Overview	35
	IPsec Configuration for an ES PIC Overview	35
	Configuring Manual SAs on an ES PIC	35
	Configuring IKE Requirements on an ES PIC	36
	Configuring a Digital Certificate for IKE on an ES PIC	36
	Configuring Security Associations for IPsec on an ES PIC	37
	Configuring the Description for an SA	38
	Configuring IPsec Transport Mode	38
	Configuring IPsec Tunnel Mode	38
	Configuring IPsec Security Associations	39
	Configuring Manual IPsec Security Associations for an ES PIC	39
	Configuring the Processing Direction	40
	Configuring the Protocol for a Manual SA	41
	Configuring the Security Parameter Index	41
	Configuring the Auxiliary Security Parameter Index	42
	Configuring the Authentication Algorithm and Key	42
	Configuring the Encryption Algorithm and Key	42
	Configuring Dynamic IPsec Security Associations	43
	Configuring an IKE Policy	44
	Configuring an IKE Policy for Preshared Keys	44
	Configuring the Description for an IKE Policy	45
	Configuring the Mode for an IKE Policy	45
	Configuring the Preshared Key for an IKE Policy	45
	Associating Proposals with an IKE Policy	45
	Example: Configuring an IKE Policy	46
	Configuring an IPsec Proposal for an ES PIC	47
	Configuring the Authentication Algorithm for an IPsec Proposal	47
	Configuring the Description for an IPsec Proposal	48
	Configuring the Encryption Algorithm for an IPsec Proposal	48
	Configuring the Lifetime for an IPsec SA	48
	Configuring the Protocol for a Dynamic IPsec SA	49
	Configuring an IPsec Policy	49
	Configuring the IPsec Policy for an ES PIC	49
	Configuring Perfect Forward Secrecy	50
	Example: Configuring an IPsec Policy	50
Chapter 4	Configuring IPsec Security Associations	53
	Overview of IPSec	53
	Security Associations Overview	53
	IKE Key Management Protocol Overview	54

	IPsec Requirements for Junos-FIPS	55
	Overview of IPsec	56
	IPsec-Enabled Line Cards	56
	Authentication Algorithms	57
	Encryption Algorithms	58
	IPsec Protocols	59
	IPsec Security Associations Overview	61
	IPsec Security Associations	61
	IPsec Modes	61
	Digital Certificates and Service Sets	62
	Digital Certificates	62
	Service Sets	64
	Configuring Security Associations	64
	Configuring Security Associations	64
	Configuring Manual SAs	64
	Configuring IKE Dynamic SAs	66
	Directing Traffic into an IPsec Tunnel	70
	Using a Filter to Select Traffic to Be Secured	70
	Applying the Filter or Service Set to the Interface Receiving Traffic to Be Secured	72
Chapter 5	Using Digital Certificates for IPsec	73
	Using Digital Certificates for IPsec	73
	Using Digital Certificates for IPsec	73
	Configuring a CA Profile	74
	Configuring a Certificate Revocation List	74
	Requesting a CA Digital Certificate	75
	Requesting a CA Digital Certificate	75
	Generating a Private/Public Key Pair	76
	Generating and Enrolling a Local Digital Certificate	76
	Applying the Local Digital Certificate to an IPsec Configuration	76
	Configuring Automatic Reenrollment of Digital Certificates	77
	Monitoring and Clearing Digital Certificates	77
	Monitoring Digital Certificates	77
	Clearing Digital Certificates	78
Chapter 6	Additional IPsec Options	79
	Using Filter-Based Forwarding to Select Traffic to Be Secured	79
	Using IPsec with a Layer 3 VPN	80
	Securing BGP Sessions with IPsec Transport Mode	82
	Securing OSPFv2 Networks with IPsec Transport Mode	83
Chapter 7	Configuring IPsec Dynamic Endpoints	85
	Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels	85
	Configuring the Service Set for IPsec Dynamic Endpoint Tunnels	86
	Configuring the Interface Identifier for IPsec Dynamic Endpoint Tunnels	87
	Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels	87
	Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels	87
	Configuring the Service Set for IPsec Dynamic Endpoint Tunnels	88
	Configuring the Interface Identifier for IPsec Dynamic Endpoint Tunnels	89

Chapter 8

Configuring Multiple Routed Tunnels in a Single Next-Hop Service Set	89
Additional ES and AS PIC Configuration Examples	93
Example: ES PIC Manual SA Configuration	93
Verifying Your Work	99
Router 1	100
Router 2	100
Router 3	101
Router 4	102
Example: AS PIC Manual SA Configuration	102
Verifying Your Work	108
Router 1	109
Router 2	109
Router 3	110
Example: ES PIC IKE Dynamic SA Configuration	111
Verifying Your Work	118
Router 1	118
Router 2	119
Router 3	120
Router 4	121
Example: AS PIC IKE Dynamic SA Configuration	122
Verifying Your Work	128
Router 1	128
Router 2	128
Router 3	129
Router 4	130
Example: IKE Dynamic SA Between an AS PIC and an ES PIC Configuration	131
Verifying Your Work	140
Router 1	140
Router 2	141
Router 3	143
Router 4	144
Example: AS PIC IKE Dynamic SA with Digital Certificates Configuration	145
Verifying Your Work	155
Router 1	155
Router 2	156
Router 3	160
Router 4	163
Example: Dynamic Endpoint Tunneling Configuration	164
Verifying Your Work	165

Part 3

Digital Certificates

Chapter 9

Configuring Digital Certificates 169

Public Key Cryptography	169
Understanding Public Key Cryptography on Switches	170
Public Key Infrastructure (PKI) and Digital Certificates	170
Understanding Self-Signed Certificates on EX Series Switches	171
Manually Generating Self-Signed Certificates on Switches (CLI Procedure)	172
Generating a Public-Private Key Pair on Switches	172
Generating Self-Signed Certificates on Switches	173
Deleting Self-Signed Certificates (CLI Procedure)	173
Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)	173
Configuring Digital Certificates	174
Digital Certificates Overview	174
Obtaining a Certificate from a Certificate Authority for an ES PIC	175
Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router	175
Example: Requesting a CA Digital Certificate	176
Generating a Private and Public Key Pair for Digital Certificates for an ES PIC	176
Configuring Digital Certificates for an ES PIC	177
Configuring the Certificate Authority Properties for an ES PIC	178
Specifying the Certificate Authority Name	178
Configuring the Certificate Revocation List	178
Configuring the Type of Encoding Your CA Supports	179
Specifying an Enrollment URL	179
Specifying a File to Read the Digital Certificate	179
Specifying an LDAP URL	179
Configuring the Cache Size	180
Configuring the Negative Cache	180
Configuring the Number of Enrollment Retries	180
Configuring the Maximum Number of Peer Certificates	181
Configuring the Path Length for the Certificate Hierarchy	181
IKE Policy for Digital Certificates on an ES PIC	182
Configuring an IKE Policy for Digital Certificates for an ES PIC	182
Configuring the Type of Encoding Your CA Supports	182
Configuring the Identity to Define the Remote Certificate Name	182
Specifying the Certificate Filename	183
Specifying the Private and Public Key File	183
Obtaining a Signed Certificate from the CA for an ES PIC	183
Associating the Configured Security Association with a Logical Interface	184
Configuring Digital Certificates for Adaptive Services Interfaces	185
Configuring the Certificate Authority Properties	186
Specifying the CA Profile Name	187
Specifying an Enrollment URL	187

Specifying the Enrollment Properties	187
Configuring the Certificate Revocation List	188
Specifying an LDAP URL	188
Configuring the Interval Between CRL Updates	189
Overriding Certificate Verification if CRL Download Fails	189
Managing Digital Certificates	189
Requesting a CA Digital Certificate for AS and Multiservices PICs installed on M Series and T Series Routers	189
Generating a Public/Private Key Pair	190
Generating and Enrolling a Local Digital Certificate	190
Configuring Auto-Reenrollment of a Router Certificate	191
Specify the Certificate ID	192
Specify the CA Profile	193
Specify the Challenge Password	193
Specify the Reenroll Trigger Time	193
Specify the Regenerate Key Pair	193
Specify the Validity Period	194
Configuring Auto-Reenrollment of a Router Certificate	194
Specify the Certificate ID	195
Specify the CA Profile	195
Specify the Challenge Password	196
Specify the Reenroll Trigger Time	196
Specify the Regenerate Key Pair	196
Specify the Validity Period	196
IPsec Tunnel Traffic Configuration	196
IPsec Tunnel Traffic Configuration Overview	197
Example: Configuring an Outbound Traffic Filter	199
Example: Applying an Outbound Traffic Filter	199
Example: Configuring an Inbound Traffic Filter for a Policy Check	200
Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check	202
ES Tunnel Interface Configuration for a Layer 3 VPN	203
Tracing Operations for Security Services	203
Configuring Tracing Operations	203
Configuring Tracing Operations for IPsec Events for Adaptive Services PICs	204

Chapter 10	Configuring SSH and SSL Router Access	207
	Configuring SSH Host Keys for Secure Copying of Data	207
	Configuring SSH Known Hosts	207
	Configuring Support for SCP File Transfer	208
	Updating SSH Host Key Information	209
	Retrieving Host Key Information Manually	209
	Importing Host Key Information from a File	209
	Importing SSL Certificates for Junos XML Protocol Support	209
	Configuring IPsec for FIPS Mode	211
	Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode	211
	Configuring the SA Direction	212
	Configuring the IPsec SPI	213
	Configuring the IPsec Key	213
	Example: Configuring Internal IPsec	214
Part 4	MACsec	
Chapter 11	Understanding MACsec	217
	Understanding Media Access Control Security (MACsec)	217
	Understanding Media Access Control Security (MACsec)	217
	How MACsec Works	218
	Understanding Connectivity Associations and Secure Channels	219
	Understanding Static Connectivity Association Key Security Mode (Security Mode for Router-to-Router Links)	219
	Understanding MACsec Hardware Requirements for MX and PTX Series Routers	220
	Understanding MACsec Software Requirements for MX Series Routers	220
	Understanding MACsec Security Modes for Switch-to-Switch Links	221
	Understanding the Requirements to Enable MACsec on a Switch-to-Host Link	223
	MACsec Software Image Requirements for EX Series and QFX Series Switches	224
	MACsec Hardware and Software Support Summary	225
	Understanding MACsec in a Virtual Chassis	227
	Understanding the MACsec Feature License Requirement	227
	MACsec Limitations	228
	Configuring MACsec on EX, SRX and Fusion Devices	228
	Acquiring and Downloading the Junos OS Software	229
	Acquiring and Downloading the MACsec Feature License	230
	Configuring the PIC Mode of the MACsec-capable Interfaces (EX4200 switches only)	231
	Configuring MACsec Using Static Connectivity Association Key Security Mode (Recommended for Enabling MACsec on Switch-to-Switch Links)	233
	Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link	238

	Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link	243
Chapter 12	MACsec Examples	249
	Configuring MACsec on EX, SRX and Fusion Devices	249
	Acquiring and Downloading the Junos OS Software	250
	Acquiring and Downloading the MACsec Feature License	251
	Configuring the PIC Mode of the MACsec-capable Interfaces (EX4200 switches only)	252
	Configuring MACsec Using Static Connectivity Association Key Security Mode (Recommended for Enabling MACsec on Switch-to-Switch Links)	254
	Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link	259
	Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link	264
	Configuring Media Access Control Security (MACsec) on MX Series Routers	268
	Configuring MACsec Using Static Connectivity Association Key Security Mode	270
	Configuring MACsec Using Preshared Key Hitless Rollover Keychain on MX-series Routers (Recommended for Enabling MACsec on Router-to-Router Links)	276
	Configuring MACsec Key Agreement Protocol in Fail Open Mode on MX2020 and MX2010 Routers	279
	Configuring MACsec with Fallback PSK	279
	Example: Configuring MACsec over an MPLS CCC on EX Series Switches	281
	Example: Configuring MACsec over an MPLS CCC on MX Series Routers	304
Part 5	MAC Limiting and Move Limiting	
Chapter 13	MAC Limiting and Move Limiting Configurations and Examples	329
	Understanding MAC Limiting and MAC Move Limiting	330
	MAC Limiting	330
	MAC Move Limiting	331

Actions for MAC Limiting and MAC Move Limiting	331
Understanding MAC Limiting on Layer 3 Routing Interfaces	332
Overview	333
Limitations	334
Understanding and Using Persistent MAC Learning	335
Understanding Persistent MAC Learning (Sticky MAC)	335
Configuring Persistent MAC Learning (ELS)	337
Configuring Persistent MAC Learning (non-ELS)	338
Verifying That Persistent MAC Learning Is Working Correctly	339
Configuring MAC Limiting	339
Configuring MAC Limiting (ELS)	339
Limiting the Number of MAC Addresses Learned by an Interface	340
Limiting the Number of MAC Addresses Learned by a VLAN	340
Configuring MAC Limiting (non-ELS)	341
Limiting the Number of MAC Addresses That Can be Learned on Interfaces	342
Specifying MAC Addresses That Are Allowed	342
Configuring MAC Limiting for VLANs	343
Configuring MAC Limiting (QFX Switches)	344
Configuring MAC Limiting (J-Web Procedure)	346
Example: Configuring MAC Limiting	347
Example: Protecting against DHCP Starvation Attacks	347
Example: Protecting against Rogue DHCP Server Attacks	351
Example: Protecting against Ethernet Switching Table Overflow Attacks	354
Verifying That MAC Limiting Is Working Correctly	357
Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly	358
Verifying That MAC Limiting for a Specific Interface Within a Specific VLAN Is Working Correctly	359
Verifying That Allowed MAC Addresses Are Working Correctly	360
Verifying Results of Various Action Settings When the MAC Limit Is Exceeded	361
Verifying That Interfaces Are Shut Down	363
Customizing the Ethernet Switching Table Display to View Information for a Specific Interface	363
Override a MAC Limit Applied to All Interfaces	364
Configuring MAC Move Limiting (ELS)	365
Verifying That MAC Move Limiting Is Working Correctly	366
Verifying That the Port Error Disable Setting Is Working Correctly	367

Part 6

Chapter 14

DHCP Protection

DHCPv4 and DHCPv6	371
Understanding and Using Trusted DHCP Servers	371
Understanding Trusted and Untrusted Ports and DHCP Servers	371
Enabling a Trusted DHCP Server (ELS)	372
Enabling a Trusted DHCP Server (non-ELS)	373

Chapter 15

Enabling a Trusted DHCP Server (MX Series Routers)	373
Verifying That a Trusted DHCP Server Is Working Correctly	374
Example: Protecting against Rogue DHCP Server Attacks	374
DHCPv6 Rapid Commit	378
Configuring DHCPv6 Rapid Commit (MX, EX)	378
Configuring the DHCPv6 Client Rapid Commit Option	378
Using Lightweight DHCPv6 Relay Agent (LDRA)	379
Configuring Persistent Bindings in the DHCP or DHCPv6 (ELS)	381
Configuring Persistent Bindings in the DHCP or DHCPv6 (non-ELS)	383
DHCP Snooping	385
Understanding DHCP Snooping (ELS)	385
DHCP Snooping Basics	386
Enabling DHCP Snooping	387
DHCP Snooping Process	387
DHCPv6 Snooping	388
Rapid Commit for DHCPv6	389
DHCP Server Access	389
Switch, DHCP Clients, and the DHCP Server Are All on the Same	
VLAN	389
Switch Acts as the DHCP Server	391
Switch Acts as a Relay Agent	391
Static IP Address Additions to the DHCP Snooping Database	392
Understanding DHCP Snooping (non-ELS)	393
DHCP Snooping Basics	393
DHCP Snooping Process	394
DHCPv6 Snooping	395
Rapid Commit for DHCPv6	396
DHCP Server Access	396
Switching Device, DHCP Clients, and DHCP Server Are All on the Same	
VLAN	396
Switching Device Acts as DHCP Server	397
Switching Device Acts as Relay Agent	398
Static IP Address Additions to the DHCP Snooping Database	399
Snooping DHCP Packets That Have Invalid IP Addresses	399
Prioritizing Snooped Packets	400
Enabling DHCP Snooping (non-ELS)	400
Enabling DHCP Snooping	401
Applying CoS Forwarding Classes to Prioritize Snooped Packets	401
Verifying That DHCP Snooping Is Working Correctly	402
Configuring Static DHCP IP Addresses	403
Configuring Static DHCP IP Addresses for DHCP snooping (ELS)	404
Configuring Static DHCP IP Addresses for DHCP snooping (non-ELS)	405
Configuring Static DHCP IP Addresses for DHCP snooping (MX routers)	406
Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks	406
Example: Protecting Against DHCP Snooping Database Attacks	415
Example: Protecting Against ARP Spoofing Attacks	418
Example: Prioritizing Snooped and Inspected Packet	423

Chapter 16	DHCP Option 82	429
	Understanding DHCP Option 82	429
	DHCP Option 82 Overview	429
	Suboption Components of Option 82	430
	Switching Device Configurations That Support Option 82	431
	Switching Device, DHCP Clients, and the DHCP Server Are on the Same VLAN or Bridge Domain	431
	Switching Device Acts as a Relay Agent	432
	DHCPv6 Options	432
	Example: Setting Up DHCP Option 82	433
	Example: Setting Up DHCP Option 82 on a VLAN	433
	Configuring DHCP Option 82 on a Router with Bridge Domain	437
	Example: Setting Up DHCP Option 82 (No Relay)	438
	Setting Up DHCP Option 82 on the Switch with No Relay (ELS)	439
	Setting Up DHCP Option 82 on the Switch with No Relay (non-ELS)	441
	Example: Setting Up DHCP Option 82 Using the Same VLAN	443
Chapter 17	Dynamic ARP Inspection (DAI)	449
	Understanding and Using Dynamic ARP Inspection (DAI)	449
	Understanding ARP Spoofing and Inspection	449
	Address Resolution Protocol	450
	ARP Spoofing	450
	Dynamic ARP Inspection	450
	Prioritizing Inspected Packets	451
	Enabling Dynamic ARP Inspection (ELS)	451
	Enabling Dynamic ARP Inspection (non-ELS)	452
	Enabling DAI on a VLAN	452
	Enabling DAI on a bridge domain	452
	Applying CoS Forwarding Classes to Prioritize Inspected Packets	453
	Verifying That DAI Is Working Correctly	453
	Configuring Static ARP Table Entries For Mapping IP Addresses to MAC Addresses	454
Part 7	IP Source Guard	
Chapter 18	Understanding IP Source Guard	459
	Understanding IP Source Guard for Port Security on Switches	459
	IP Address Spoofing	459
	How IP Source Guard Works	459
	IPv6 Source Guard	460
	The DHCP Snooping Table	460
	Typical Uses of Other Junos OS Features with IP Source Guard	461
	Configuring IP Source Guard (non-ELS)	461
	Configuring IP Source Guard	462
	Configuring IPv6 Source Guard	463
	Disabling IP Source Guard	464
	Configuring IP Source Guard (ELS)	465
	Verifying That IP Source Guard Is Working Correctly	466

Chapter 19	IP Source Guard Examples	467
	Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN	467
	Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces	476
	Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing	487
	Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing	492
	Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing	497
	Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks	497
	Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing	502
 Part 8	 IPv6 Access Security	
Chapter 20	Neighbor Discovery Protocol	509
	IPv6 Neighbor Discovery Inspection	509
	IPv6 Neighbor Discovery Protocol Overview	509
	Neighbor Discovery (ND) Inspection	509
	Enabling ND Inspection	510
Chapter 21	Router Advertisement Guard	511
	Understanding IPv6 Router Advertisement Guard	511
	Configuring Stateful IPv6 Router Advertisement Guard	514
	Enabling Stateful RA Guard on an Interface	515
	Enabling Stateful RA Guard on a VLAN	515
	Configuring the Learning State on an Interface	516
	Configuring the Forwarding State on an Interface	517
	Configuring the Blocking State on an Interface	517
	Configuring Stateless IPv6 Router Advertisement Guard	517
	Configuring a Discard Policy for RA Guard	518
	Configuring an Accept Policy for RA Guard	519
	Enabling Stateless RA Guard on an Interface	521
	Enabling Stateless RA Guard on a VLAN	522
	Configuring an Interface as Trusted or Blocked to Bypass Inspection by RA Guard	522
 Part 9	 Distributed Denial-of-Service (DDoS) Protection	
Chapter 22	DDoS Protection	527
	Distributed Denial-of-Service (DDoS) Protection Overview	527
	Host-bound Traffic Policers for DDoS Violations	527
	Platform Support	529
	Policer Types and Packet Priorities	530
	Example of Policer Priority Behavior	530
	Policer Hierarchy on Routers	531
	Example of Policer Bandwidth Limit Behavior	533

DDoS Protection Compared to Subscriber Login Packet Overload Protection	534
Configuring DDoS Protection	535
Disabling DDoS Protection Policers and Logging Globally	536
Configuring DDoS Protection Aggregate or Individual Packet Type Policers	537
Verifying and Managing DDoS Protection	542
Tracing DDoS Protection Operations	543
Configuring the DDoS Protection Trace Log Filename	544
Configuring the Number and Size of DDoS Protection Log Files	544
Configuring Access to the DDoS Protection Log File	544
Configuring a Regular Expression for DDoS Protection Messages to Be Logged	545
Configuring the DDoS Protection Tracing Flags	545
Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged	545
Example: Configuring DDoS Protection	546
Example: Configuring DDoS Protection on QFX Series Switches	556
Rate Limiting ICMPv4 and ICMPv6 Traffic	560

Part 10

Chapter 23

Flow Detection

Flow Detection and Culprit Flows	565
DDoS Protection Flow Detection Overview	565
Flow Detection and Control	565
Flow Tracking	566
Notifications	567
Setting Up and Using Flow Detection	568
Configuring the Detection Period for Suspicious Flows	569
Configuring the Recovery Period for a Culprit Flow	569
Configuring the Timeout Period for a Culprit Flow	570
Configuring How Flow Detection Operates at Each Flow Aggregation Level	571
Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level	572
Enabling Flow Detection for All Protocol Groups and Packet Types	573
Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types	574
Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types	574
Disabling Automatic Logging of Culprit Flow Events for a Packet Type	574
Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level	575
Verifying and Managing Flow Detection	575
Configuring How Flow Detection Operates Globally	576
Configuring How Traffic in a Culprit Flow Is Controlled Globally	578

Part 11	Unicast Forwarding	
Chapter 24	Unicast Reverse Path Forwarding	583
	Understanding Unicast RPF (Switches)	584
	Unicast RPF for Switches Overview	585
	Unicast RPF Implementation	585
	Unicast RPF Packet Filtering	585
	Bootstrap Protocol (BOOTP) and DHCP Requests	585
	Default Route Handling	585
	When to Enable Unicast RPF	586
	When Not to Enable Unicast RPF	587
	Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches	588
	Understanding Unicast RPF (Routers)	588
	Unicast RPF and Default Route	589
	Unicast RPF Behavior with a Default Route	590
	Unicast RPF Behavior Without a Default Route	590
	Unicast RPF with Routing Asymmetry	591
	Configuring Unicast RPF Strict Mode	591
	Configuring Unicast RPF Loose Mode	593
	Configuring Unicast RPF Loose Mode with Ability to Discard Packets	595
	Configuring Unicast RPF on a VPN	596
	Configuring Unicast RPF	597
	Example: Configuring Unicast RPF (On a Switch)	598
	Example: Configuring Unicast RPF (On a Router)	603
Chapter 25	Unknown Unicast Forwarding	613
	Understanding and Preventing Unknown Unicast Forwarding	613
	Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface	613
	Configuring Unknown Unicast Forwarding (ELS)	614
	Configuring Unknown Unicast Forwarding on EX4300 Switches	615
	Configuring Unknown Unicast Forwarding on EX9200 Switches	615
	Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface	617
	Configuring Unknown Unicast Forwarding (CLI Procedure)	618
Part 12	Storm Control	
Chapter 26	Understanding and Using Storm Control	621
	Understanding Storm Control	622
	Enabling and Disabling Storm Control (non-ELS)	626
	Disabling Storm Control on Broadcast Traffic	628
	Disabling Storm Control on All Multicast Traffic	628
	Disabling Storm Control on Registered Multicast Traffic (EX8200 Switches Only)	628
	Disabling Storm Control on Unregistered Multicast Traffic (EX8200 Switches Only)	628
	Disabling Storm Control on Unknown Unicast Traffic	629

Enabling Storm Control on Multicast Traffic	629
Enabling and Disabling Storm Control (ELS)	630
Configuring Storm Control	631
Disabling Storm Control on Broadcast Traffic	631
Disabling Storm Control on All Multicast Traffic	632
Disabling Storm Control on Registered Multicast Traffic	632
Disabling Storm Control on Unregistered Multicast Traffic	633
Disabling Storm Control on Unknown Unicast Traffic	633
Disabling Storm Control on Multiple Types of Traffic	634
Configuring Autorecovery for Port Security Events	635
Example: Using Storm Control to Prevent Network Outages	636
Example: Using Storm Control to Prevent Network Outages (ELS)	637
Example: Using Storm Control to Prevent Network Outages (non-ELS)	638
Example: Using Storm Control to Prevent Network (MX Routers)	641

Part 13

Chapter 27

Configuration Statements and Operational Commands

Configuration Statements	649
Security Services Configuration Statements	658
accept	660
accept-source-mac	662
access-security	664
action-priority	666
action-shutdown	667
algorithm (Authentication Keychain)	669
algorithm (Junos FIPS)	669
allowed-mac	670
arp-inspection	671
arp-inspection (MX Series)	672
authentication (Security IPsec)	673
authentication-algorithm (Security IKE)	674
authentication-algorithm (Security IPsec)	675
authentication-key-chains	677
authentication-method	678
auto-re-enrollment	679
auxiliary-spi (Security IPsec)	680
bandwidth	681
bandwidth (DDoS)	682
bandwidth-level	683
bandwidth-percentage	685
bandwidth-scale (DDoS)	686
bridge-domains	687
burst (DDoS)	688
burst-scale (DDoS)	689
bypass-aggregate (DDoS)	690
cache-size	691
cache-timeout-negative	692
ca-identity	693
cak	694

cak (MX Series)	695
ca-name	696
ca-profile (Security PKI)	697
certificate-id	698
certificates	699
certification-authority	700
challenge-password	701
children	702
cipher-suite (MACsec)	704
circuit-id	706
ckn	707
connections (Host VPN)	708
connectivity-association	710
connectivity-association (MACsec Interfaces)	711
connectivity-association (MACsec Interfaces for MX Series)	712
crl (Adaptive Services Interface)	713
crl (Encryption Interface)	714
ddos-protection (DDoS)	715
description (Authentication Keychain)	718
description (IKE policy)	719
dhcp-option82	720
dhcp-security	721
dhcp-security (MX Series)	724
dhcp-service	726
dhcp-snooping-file	728
dhcp-snooping-file	729
dhcp-trusted	730
dhcpv6-options	731
dhcpv6-snooping-file	732
dh-group	733
direction	734
direction (Junos OS)	735
direction (Junos-FIPS Software)	736
direction (MX Series)	737
disable-fpc (DDoS)	738
disable-logging (DDoS)	739
disable-preceding-key	740
disable-routing-engine (DDoS)	741
disable-timeout	742
disable-timeout (Port Error Disable)	743
discard	744
dynamic	745
encoding	746
encryption (MACsec)	747
encryption (MACsec for MX Series)	748
encryption (Junos OS)	749
encryption (Junos-FIPS Software)	750
encryption-algorithm (Security)	751
enrollment	752

enrollment-retry	753
enrollment-url	754
ethernet-switching-options	755
examine-dhcp	761
examine-dhcpv6	763
examine-fip	765
exclude-protocol	766
exclude-protocol (MX Series)	767
fallback-key	768
family vpls (Layer 2 Pseudowires)	769
fc-map	770
fcoe-trusted	772
file	773
flood (VLANs)	774
flow-detection (DDoS Flow Detection)	775
flow-detection (DDoS Packet Level)	776
flow-detection-mode (DDoS Flow Detection)	777
flow-detection-mode (DDoS Global Flow Detection)	778
flow-detect-time (DDoS Flow Detection)	779
flow-level-bandwidth (DDoS Flow Detection)	780
flow-level-control (DDoS Flow Detection)	781
flow-level-control (DDoS Global Flow Detection)	782
flow-level-detection (DDoS Flow Detection)	783
flow-recover-time (DDoS Flow Detection)	784
flow-report-rate (DDoS Flow Detection)	785
flow-timeout-time (DDoS Flow Detection)	786
forwarding-class (for DHCP Snooping or DAI Packets)	787
forwarding-options	788
fpc (DDoS)	794
global (DDoS)	795
group (DHCP Security)	796
group (DHCP Security for MX Series)	797
group-type (Unknown Unicast Forwarding)	798
host-name	799
host-vpn	800
id	801
id (MACsec for MX Series)	802
identity	802
ike (Security)	803
ike-log	804
ike-secrets	805
include-sci	806
include-sci (MACsec for MX Series)	807
interface (Access Port Security)	808
interface (DHCP Security for MX Series)	809
interface (RA Guard)	810
interface (Secure Access Port)	811
interface (Static MAC Bypass)	812
interface (Storm Control)	813

interface (Unknown Unicast Forwarding)	814
interface-mac-limit	815
interface-shutdown-action	817
interfaces (MACsec)	818
interfaces (MACsec for MX Series)	819
internal	820
ipsec (Security)	821
ip-source-guard	823
ip-source-guard (MX Series)	825
source-ip-address-list	826
ipv6-source-guard	827
ipv6-source-guard-sessions	828
key (Authentication Keychain)	829
key (Junos FIPS)	830
key (MACsec)	831
key-chain (Security)	832
key-server-priority (MACsec)	833
key-server-priority (MACsec for MX Series)	834
ldap-url	835
level	836
lifetime-seconds (Security)	837
light-weight-dhcpv6-relay	838
local	840
local-certificate (Security)	841
local-key-pair	841
local-traffic-selector	842
location	843
location (DHCP Snooping Database)	844
logical-interface (DDoS Flow Detection)	845
mac	847
mac (Option 82)	848
mac-address (MACsec)	849
mac-address (MACsec)	850
mac-limit	851
mac-limit (Access Port Security)	852
mac-list	853
mac-move-limit	854
macsec	856
macsec (MX Series)	858
manual (Junos OS)	859
manual (Junos-FIPS Software)	860
mark-interface (RA Guard)	861
match-list	862
match-option	864
maximum-certificates	865
mka	866
mka (MX Series)	867
mode (IKE)	868
mode (IPsec)	869

multicast	870
must-secure	871
neighbor-discovery-inspection	872
next-hop-group (Unknown Unicast Forwarding)	873
no-allowed-mac-log	874
no-broadcast	875
no-dhcp-snooping	877
no-dhcp-trusted	878
no-dhcpv6-options	879
no-dhcpv6-snooping	879
no-encryption (MACsec)	880
no-encryption (MACsec for MX Series)	881
no-examine-dhcpv6	882
no-fcoe-trusted	883
no-flow-logging (DDoS Flow Detection)	884
no-gratuitous-arp-request	885
no-gratuitous-arp-request	886
no-multicast	887
no-option16	888
no-option18	889
no-option37	889
no-option82	890
no-registered-multicast	891
no-unknown-unicast	892
no-unregistered-multicast	894
offset	895
offset (MX Series)	897
option-16 (DHCPv6 Snooping)	898
option-18 (DHCPv6 Snooping)	899
option-37 (DHCPv6 Snooping)	901
no-option-37	902
option-82	903
options (Security)	904
overrides (DHCP Security)	905
overrides (DHCP Security for MX Series)	906
packet-action	907
path-length	910
perfect-forward-secrecy (Security)	911
perfect-forward-secrecy (Services)	912
persistent-learning	913
persistent-learning	914
physical-interface (DDoS Flow Detection)	915
pki	917
policy	919
policy (Security IKE)	920
policy (Security IPsec)	921
port-error-disable	922
port-id	923
port-id (MACsec for MX Series)	924

prefix (Circuit ID for Option 82)	925
prefix (DHCPv6 Options)	927
prefix (Remote ID for Option 82)	928
prefix-list-name	929
pre-shared-key	930
pre-shared-key (MX Series)	931
pre-shared-key (Security)	932
priority (DDoS)	933
proposal (Security IKE)	934
proposal (Security IPsec)	935
proposals	936
protocol (Junos OS)	937
protocol (Junos-FIPS Software)	938
protocols (DDoS)	939
protocols (DDoS) (PTX Series and QFX Series)	950
recover-time (DDoS)	958
recovery-timeout	959
re-enroll-trigger-time-percentage	960
refresh-interval	961
re-generate-keypair	961
remote (Host VPN)	962
remote-id	963
remote-id (MX Series)	965
replay-protect	966
replay-protect (MX Series)	967
remote-traffic-selector	968
replay-window-size (MX Series)	969
replay-window-size	970
retry (Adaptive Services Interface)	971
retry-interval	972
revocation-check	973
router-advertisement-guard	974
routing-instance-name	976
routing-instance-name (circuit-id)	976
rpf-check	977
secret	978
secure-access-port	979
secure-channel	981
secure-channel	982
security	983
security-association	985
security-association (Junos OS)	986
security-association (Junos-FIPS Software)	987
security-mode	988
show ddos-protection protocols culprit-flows	990
show ddos-protection protocols flow-detection	997
source-mac-address-list	1001
spi (Junos OS)	1002
spi (Junos-FIPS Software)	1003

ssh	1004
ssh-known-hosts	1006
start-time (Authentication Key Transmission)	1008
stateful	1010
stateless	1011
static-ip	1012
static-ip (MX Series)	1013
static-ipv6	1014
storm-control	1015
storm-control	1016
storm-control	1017
storm-control-profiles	1018
subscriber (DDoS Flow Detection)	1019
switch-options (VLANs)	1021
timeout	1023
timeout-active-flows (DDoS Flow Detection)	1024
tolerance	1025
traceoptions	1026
traceoptions (Access Port Security)	1028
traceoptions (DDoS)	1031
traceoptions (DHCP)	1033
traceoptions (MACsec)	1036
traceoptions (MACsec interfaces)	1038
transmit-interval (MACsec)	1040
transmit-interval (MACsec for MX Series)	1041
trusted	1042
trusted (DHCP Security)	1042
unknown-unicast-forwarding	1043
untrusted	1044
untrusted	1045
url (Security)	1046
use-interface-description	1047
use-interface-description	1049
use-interface-index	1051
use-interface-name	1052
use-string	1053
use-vlan-id	1054
validity-period	1055
vendor-id	1056
violation-report-rate (DDoS Flow Detection)	1057
vlan (Access Port Security)	1058
vlan (DHCP Bindings on Access Ports)	1060
vlan (RA Guard)	1061
vlan (Secure Access Port)	1062
vlan (Static IP)	1063
vlan (Unknown Unicast Forwarding)	1064
voip-mac-exclusive	1065
write-interval	1066

Chapter 28	Operational Commands	1067
	clear security host-vpn security-associations	1070
	clear security pki certificate-request	1071
	clear access-security router-advertisement statistics	1072
	clear arp	1073
	clear arp inspection statistics	1075
	clear bridge recovery-timeout	1076
	clear ddos-protection protocols	1077
	clear dhcp snooping binding	1079
	clear dhcp snooping statistics	1080
	clear dhcp-security binding	1081
	clear dhcp-security ipv6 binding	1082
	clear dhcpv6 snooping binding	1083
	clear dhcpv6 snooping statistics	1084
	clear dot1x	1085
	clear ethernet-switching port-error	1087
	clear ethernet-switching recovery-timeout	1088
	clear ethernet-switching table	1089
	clear neighbor-discovery-inspection statistics	1091
	show security macsec connections	1092
	clear security mka statistics	1094
	clear security mka statistics (MX Series)	1095
	clear security pki ca-certificate	1096
	clear security pki crl	1097
	clear security pki key-pair	1098
	clear security pki local-certificate	1099
	clear services ipsec-vpn certificates	1100
	clear services ipsec-vpn ike security-associations	1101
	clear services ipsec-vpn ipsec security-associations	1102
	clear services ipsec-vpn ipsec statistics	1103
	request access-security router-advertisement-guard-block	1104
	request access-security router-advertisement-guard-forward	1105
	request access-security router-advertisement-guard-learn interface	1106
	request ipsec switch	1108
	request security certificate enroll (Signed)	1109
	request security certificate enroll (Unsigned)	1111
	request security key-pair	1112
	request security pki ca-certificate enroll	1113
	request security pki ca-certificate load	1114
	request security pki ca-certificate verify	1115
	request security pki crl load	1116
	request security pki generate-certificate-request	1117
	request security pki generate-key-pair	1119
	request security pki local-certificate enroll	1120
	request security pki local-certificate generate-self-signed	1122
	request security pki local-certificate load	1123
	request security pki local-certificate verify	1124
	request system certificate add	1125
	show access-security router-advertisement state	1126

show access-security router-advertisement statistics	1128
show arp inspection statistics	1130
show ddos-protection protocols	1132
show ddos-protection protocols parameters	1153
show ddos-protection protocols statistics	1160
show ddos-protection protocols violations	1171
show ddos-protection statistics	1174
show ddos-protection version	1176
show dhcp snooping binding	1178
show dhcp snooping statistics	1180
show dhcp-security arp inspection statistics	1181
show dhcp-security binding	1183
show dhcp-security binding ip-source-guard	1186
show dhcp-security ipv6 binding	1188
show dhcp-security ipv6 statistics	1190
show dhcp-security neighbor-discovery-inspection statistics	1193
show dhcpv6 snooping binding	1195
show dhcpv6 snooping statistics	1197
show ethernet-switching table	1198
show ike security-associations	1221
show ipsec certificates	1225
show ipsec security-associations	1228
show ip-source-guard	1231
show ipv6-source-guard	1233
show neighbor-discovery-inspection statistics	1235
show security host-vpn security-associations	1236
show security host-vpn version	1239
show security keychain	1240
show security macsec connections (MX Series)	1243
show security macsec statistics	1246
include-sci (MACsec for MX Series)	1250
show security mka sessions	1251
show security mka sessions (MX Series)	1253
show security mka sessions summary	1257
show security mka statistics	1258
show security pki ca-certificate	1260
show security pki certificate-request	1264
show security pki crl	1267
show security pki local-certificate	1270
show services ipsec-vpn certificates	1273
show services ipsec-vpn ike security-associations	1276
show services ipsec-vpn ipsec security-associations	1281
show services ipsec-vpn ipsec statistics	1287
show system certificate	1291
show system statistics arp	1293

List of Figures

Part 1	Port Security	
Chapter 1	Port Security Overview	3
	Figure 1: Network Topology for Basic Port Security	16
Part 2	IPSec	
Chapter 4	Configuring IPsec Security Associations	53
	Figure 2: AH Protocol	59
	Figure 3: ESP Protocol	60
Chapter 8	Additional ES and AS PIC Configuration Examples	93
	Figure 4: ES PIC Manual SA Topology Diagram	93
	Figure 5: AS PIC Manual SA Topology Diagram	102
	Figure 6: ES PIC IKE Dynamic SA Topology Diagram	111
	Figure 7: AS PIC IKE Dynamic SA Topology Diagram	122
	Figure 8: AS PIC to ES PIC IKE Dynamic SA Topology Diagram	131
	Figure 9: AS PIC IKE Dynamic SA Topology Diagram	145
	Figure 10: IPsec Dynamic Endpoint Tunneling Topology Diagram	164
Part 3	Digital Certificates	
Chapter 9	Configuring Digital Certificates	169
	Figure 11: Example: IPsec Tunnel Connecting Security Gateways	197
Part 4	MACsec	
Chapter 12	MACsec Examples	249
	Figure 12: MPLS Diagram Between Site A and Site B	283
Part 5	MAC Limiting and Move Limiting	
Chapter 13	MAC Limiting and Move Limiting Configurations and Examples	329
	Figure 13: Network Topology for Basic Port Security	348
	Figure 14: Network Topology for Basic Port Security	352
	Figure 15: Network Topology for Basic Port Security	355
Part 6	DHCP Protection	
Chapter 14	DHCPv4 and DHCPv6	371
	Figure 16: Network Topology for Basic Port Security	376
Chapter 15	DHCP Snooping	385

	Figure 17: DHCP Server Connected Directly to a Switch	390
	Figure 18: DHCP Server Connected Directly to Switch 2, with Switch 2 Connected to Switch 1 Through a Trusted Trunk Port	390
	Figure 19: Switch Is the DHCP Server	391
	Figure 20: Switch Acting as a Relay Agent Through a Router to the DHCP Server	392
	Figure 21: DHCP Server Connected Directly to a Switching Device	397
	Figure 22: DHCP Server Connected Directly to Switching Device 2, with Switching Device 2 Connected to Switching Device 1 Through a Trusted Trunk Port	397
	Figure 23: Switching Device Is the DHCP Server	398
	Figure 24: Switching Device Acting as Relay Agent Through Router to DHCP Server	399
	Figure 25: Network Topology for Port Security Setup with Two Switches on the Same VLAN	408
	Figure 26: Network Topology for Basic Port Security	416
	Figure 27: Network Topology for Basic Port Security	420
	Figure 28: Network Topology for Using CoS Forwarding Classes to Prioritize Snooped and Inspected Packets	424
Chapter 16	DHCP Option 82	429
	Figure 29: DHCP Clients, Switching Device, and the DHCP Server Are All on the Same VLAN or Bridge Domain	431
	Figure 30: Switching Device Acting as an Extended Relay Server	432
	Figure 31: Network Topology for Configuring DHCP Option 82 on a Switch That Is on the Same VLAN as the DHCP Clients and the DHCP Server	445
Part 7	IP Source Guard	
Chapter 19	IP Source Guard Examples	467
	Figure 32: Network Topology for Basic Port Security	489
	Figure 33: Network Topology for Basic Port Security	494
	Figure 34: Switching Device Network Topology for Basic Port Security	499
	Figure 35: Network Topology for Basic Port Security	503
Part 8	IPv6 Access Security	
Chapter 21	Router Advertisement Guard	511
	Figure 36: Stateful RA Guard State Transitions	513
Part 9	Distributed Denial-of-Service (DDoS) Protection	
Chapter 22	DDoS Protection	527
	Figure 37: Policer Hierarchy for PPPoE Packets	531
	Figure 38: Policer Hierarchy for DHCPv4 Packets	532
Part 11	Unicast Forwarding	
Chapter 24	Unicast Reverse Path Forwarding	583
	Figure 39: Symmetrically Routed Interfaces	586
	Figure 40: Asymmetrically Routed Interfaces	587

	Figure 41: Unicast RPF with Routing Asymmetry	591
	Figure 42: Unicast RPF Sample Topoolgy	604
Part 12	Storm Control	
Chapter 26	Understanding and Using Storm Control	621
	Figure 43: Example Storm Control to Prevent Network Outages	642

List of Tables

	About the Documentation	xxxv
	Table 1: Notice Icons	xxxvii
	Table 2: Text and Syntax Conventions	xxxviii
Part 1	Port Security	
Chapter 1	Port Security Overview	3
	Table 3: Components of the Port Security Topology	16
Part 2	IPSec	
Chapter 3	IPsec Configurations and Examples	31
	Table 4: Comparison of IPsec Configuration Statements and Operational Mode Commands for the AS and MultiServices PICs and ES PIC	31
	Table 5: Authentication and Encryption Key Lengths	33
	Table 6: Weak and Semiweak Keys	34
Chapter 4	Configuring IPsec Security Associations	53
	Table 7: IKE and IPsec Proposal and Policy Default Values for the AS and MultiServices PICs	67
Part 4	MACsec	
Chapter 11	Understanding MACsec	217
	Table 8: Line cards and MICs supporting MACsec on MX series and PTX series Routers	220
	Table 9: MACsec Hardware and Software Support Summary for EX Series and QFX Series Switches	225
Chapter 12	MACsec Examples	249
	Table 10: CAK status descriptions	280
	Table 11: Components of the MPLS Topology	284
	Table 12: MACsec Connectivity Association Summary	285
	Table 13: VLANs Summary	285
	Table 14: Components of the MPLS Topology	305
	Table 15: MACsec Connectivity Association Summary	306
	Table 16: Bridge Domains Summary	307
Part 5	MAC Limiting and Move Limiting	
Chapter 13	MAC Limiting and Move Limiting Configurations and Examples	329
	Table 17: Components of the Port Security Topology	348

	Table 18: Components of the Port Security Topology	352
	Table 19: Components of the Port Security Topology	355
Part 6	DHCP Protection	
Chapter 14	DHCPv4 and DHCPv6	371
	Table 20: Components of the Port Security Topology	376
Chapter 15	DHCP Snooping	385
	Table 21: DHCPv6 Messages and DHCPv4 Equivalent Messages	388
	Table 22: DHCPv6 Messages and Equivalent DHCPv4 Messages	395
	Table 23: Components of Port Security Setup on Switch 1 with a DHCP Server Connected to Switch 2	408
	Table 24: Components of the Port Security Topology	416
	Table 25: Components of the Port Security Topology	420
	Table 26: Components of the Topology for Using CoS Forwarding Classes to Prioritize Snooped and Inspected Packets	425
Part 7	IP Source Guard	
Chapter 19	IP Source Guard Examples	467
	Table 27: Components of the Port Security Topology	489
	Table 28: Components of the Port Security Topology	494
	Table 29: Components of the Port Security Topology	499
	Table 30: Components of the Port Security Topology	504
Part 8	IPv6 Access Security	
Chapter 21	Router Advertisement Guard	511
	Table 31: IPv6 RA guard states	512
Part 10	Flow Detection	
Chapter 23	Flow Detection and Culprit Flows	565
	Table 32: Triggering Event for Flow Detection Reports	567
	Table 33: Triggering Event for Bandwidth Violation Reports	568
Part 13	Configuration Statements and Operational Commands	
Chapter 27	Configuration Statements	649
	Table 34: Security Services Configuration Statements	658
	Table 35: Unified Forwarding Table Profiles	792
	Table 36: Packet Types Supported by DDoS Protection on PTX Series routers and QFX Series Switches	952
	Table 37: Protocol Groups Supported by DDoS Protection on QFX Switches	954
	Table 38: show ddos-protection protocols culprit-flows Output Fields	991
	Table 39: show ddos-protection protocols flow-detection Output Fields	998
Chapter 28	Operational Commands	1067
	Table 40: show security macsec connections Output Fields	1092
	Table 41: show access-security router-advertisement state Output Fields	1126

Table 42: show access-security router-advertisement statistics Output Fields	1128
Table 43: show arp inspection statistics Output Fields	1130
Table 44: Supported Protocol Groups	1137
Table 45: show ddos-protection protocols Output Fields	1143
Table 46: show ddos-protection protocols parameters Output Fields	1154
Table 47: show ddos-protection protocols statistics Output Fields	1161
Table 48: show ddos-protection protocols violations Output Fields	1172
Table 49: show ddos-protection statistics Output Fields	1174
Table 50: show ddos-protection version Output Fields	1176
Table 51: show dhcp snooping binding Output Fields	1178
Table 52: show dhcp snooping statistics Output Fields	1180
Table 53: show dhcp-security arp inspection statistics Output Fields	1181
Table 54: show dhcp-security binding Output Fields	1184
Table 55: show dhcp-security binding ip-source-guard Output Fields	1186
Table 56: show dhcp-security ipv6 binding Output Fields	1189
Table 57: show dhcp-security ipv6 statistics Output Fields	1191
Table 58: show dhcp-security neighbor-discovery-inspection statistics Output Fields	1193
Table 59: show dhcp snooping binding Output Fields	1195
Table 60: show dhcpv6 snooping statistics Output Fields	1197
Table 61: show ethernet-switching table Output Fields	1201
Table 62: show ethernet-switching table Output Fields	1202
Table 63: show ethernet-switching table Output fields	1202
Table 64: show ethernet-switching table Output Fields	1203
Table 65: show ike security-associations Output Fields	1221
Table 66: show ipsec certificates Output Fields	1225
Table 67: show ipsec security-associations Output Fields	1228
Table 68: show ip-source-guard Output Fields	1231
Table 69: show ipv6-source-guard Output Fields	1233
Table 70: show neighbor-discovery-inspection statistics Output Fields	1235
Table 71: show security host-vpn security-associations Output Fields	1236
Table 72: show security keychain Output Fields	1240
Table 73: show security macsec connections Output Fields	1243
Table 74: show security macsec statistics Output Fields	1247
Table 75: show security mka sessions Output Fields	1251
Table 76: show security mka sessions Output Fields	1253
Table 77: show security mka sessions summary Output Fields	1257
Table 78: show security mka statistics Output Fields	1258
Table 79: show security pki ca-certificate Output Fields	1260
Table 80: show security pki certificate-request Output Fields	1264
Table 81: show security pki crl Output Fields	1267
Table 82: show security pki local-certificate Output Fields	1270
Table 83: show services ipsec-vpn certificates Output Fields	1273
Table 84: show services ipsec-vpn ike security-associations Output Fields	1276
Table 85: show services ipsec-vpn ipsec security-associations Output Fields	1281
Table 86: show services ipsec-vpn ipsec statistics Output Fields	1287
Table 87: show system certificate Output Fields	1291

About the Documentation

- Documentation and Release Notes on page xxxv
- Using the Examples in This Manual on page xxxv
- Documentation Conventions on page xxxvii
- Documentation Feedback on page xxxix
- Requesting Technical Support on page xxxix

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 <https://www.juniper.net/documentation/>.

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 <https://www.juniper.net/books>.

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 xxxvii 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 xxxviii 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 <i>metric</i> >;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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 [<i>community-ids</i>]
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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide 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 Juniper Care or Partner Support Services 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 <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- 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 <https://support.juniper.net/support/requesting-support/>.

PART 1

Port Security

- [Port Security Overview on page 3](#)

CHAPTER 1

Port Security Overview

- [Overview of Port Security on page 3](#)

Overview of Port Security

- [Port Security Features on page 3](#)
- [Understanding How to Protect Access Ports from Common Attacks on page 6](#)
- [Configuring Port Security \(ELS\) on page 9](#)
- [Configuring Port Security \(non-ELS\) on page 11](#)
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)

Port Security Features

Ethernet LANs are vulnerable to attacks such as address spoofing (forging) and Layer 2 denial of service (DoS) on network devices. Port security features help protect the access ports on your device against the loss of information and productivity that such attacks can cause.

Junos OS is hardened through the separation of control forwarding and services planes, with each function running in protected memory. The control-plane CPU is protected by rate limiting, routing policy, and firewall filters to ensure switch uptime even under severe attack.

Junos OS provides features to help secure ports on a device. Ports can be categorized as either trusted or untrusted. You apply policies appropriate to each category to protect ports against various types of attacks.

Access port security features such as dynamic Address Resolution Protocol (ARP) inspection, DHCP snooping, and MAC limiting are controlled through a single Junos OS CLI command. Basic port security features are enabled in the device's default configuration. You can configure additional features with minimal configuration steps.

Depending on the particular feature, you can configure the feature either on VLANs or bridge domain interfaces.

Juniper Networks EX Series Ethernet Switches provide the following hardware and software security features:

Console Port—Allows use of the console port to connect to the Routing Engine through an RJ-45 cable. You then use the command-line interface (CLI) to configure the switch.

Out-of-Band Management—A dedicated management Ethernet port on the rear panel allows out-of-band management.

Software Images—All Junos OS images are signed by Juniper Networks certificate authority (CA) with public key infrastructure (PKI).

User Authentication, Authorization, and Accounting (AAA)—Features include:

- User and group accounts with password encryption and authentication.
- Access privilege levels configurable for login classes and user templates.
- RADIUS authentication, TACACS+ authentication, or both, for authenticating users who attempt to access the switch.
- Auditing of configuration changes through system logging or RADIUS/TACACS+.

802.1X Authentication—Provides network access control. Supplicants (hosts) are authenticated when they initially connect to a LAN. Authenticating supplicants before they receive an IP address from a DHCP server prevents unauthorized supplicants from gaining access to the LAN. EX Series switches support Extensible Authentication Protocol (EAP) methods, including EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP.

Port Security—Access Port security features supported on switching devices are::

- DHCP snooping—Filters and blocks ingress Dynamic Host Configuration Protocol (DHCP) server messages on untrusted ports, and builds and maintains a database of DHCP lease information, which is called the DHCP snooping database.



NOTE: DHCP snooping is not enabled in the default configuration of the switching device. DHCP snooping is enabled on a VLAN or bridge domain. The details of enabling DHCP snooping depend on the particular device.

- Trusted DHCP server—Configuring the DHCP server on a trusted port protects against rogue DHCP servers sending leases. You enable this feature on an interface (port). By default, access ports are untrusted, and trunk ports are trusted. (Access ports are the switch ports that connect to Ethernet endpoints such as user PCs and laptops, servers, and printers. Trunk ports are the switch ports that connect an Ethernet switch to other switches or to routers.)
- DHCPv6 snooping—DHCP snooping for IPv6.
- DHCP option 82—Also known as the DHCP Relay Agent Information option. This DHCPv4 feature helps protect the switching device against attacks such as spoofing of IP addresses and MAC addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.

- DHCPv6 option 37—Option 37 is the remote ID option for DHCPv6 and is used to insert information about the network location of the remote host into DHCPv6 packets. You enable option 37 on a VLAN.



NOTE: DHCPv6 snooping with option 37 is not supported on the MX Series.

- DHCPv6 option 18—Option 18 is the circuit ID option for DHCPv6 and is used to insert information about the client port into DHCPv6 packets. This option includes other details that can be optionally configured, such as the prefix and the interface description.
- DHCPv6 option 16—Option 16 is the vendor ID option for DHCPv6 and is used to insert information about the vendor of the client hardware into DHCPv6 packets.
- Dynamic ARP inspection (DAI)—Prevents Address Resolution Protocol (ARP) spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable DAI on a VLAN.
- IPv6 neighbor discovery inspection—Prevents IPv6 address spoofing attacks. Neighbor discovery requests and replies are compared against entries in the DHCPv6 snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable neighbor discovery inspection on a VLAN.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. With IP source guard enabled, the source IP address in the packet sent from an untrusted access interface is validated against the DHCP snooping database. If the packet cannot be validated, it is discarded. You enable IP source guard on a VLAN or bridge domain.



NOTE: IP source guard is not supported on the QFX Series.

- IPv6 source guard—IP source guard for IPv6.



NOTE: IPv6 source guard is not supported on the QFX Series.

- MAC limiting—Protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You can enable MAC limiting on an interface.
- MAC move limiting—Tracks MAC movement and detects MAC spoofing on access ports. You enable this feature on a VLAN or bridge domain.
- Persistent MAC learning—Also known as sticky MAC. Persistent MAC learning enables interfaces to retain dynamically learned MAC addresses across switch reboots. You enable this feature on an interface.
- Unrestricted proxy ARP—The switch responds to all ARP messages with its own MAC address. Hosts that are connected to the switch's interfaces cannot communicate

directly with other hosts. Instead, all communications between hosts go through the switch.

- **Restricted proxy ARP**—The switch does not respond to an ARP request if the physical networks of the source and target of the ARP request are the same. It does not matter whether the destination host has the same IP address as the incoming interface or a different (remote) IP address. An ARP request for a broadcast address elicits no reply.

Device Security—Storm control permits the switch to monitor unknown unicast and broadcast traffic and drop packets, or shut down, or temporarily disable the interface when a specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. You can enable storm control on access interfaces or trunk interfaces.

Encryption Standards—Supported standards include:

- 128-, 192-, and 256-bit Advanced Encryption Standard (AES)
- 56-bit Data Encryption Standard (DES) and 168-bit 3DES

- See Also**
- [Understanding DHCP Snooping \(non-ELS\) on page 393](#)
 - [Understanding DHCP Snooping \(ELS\) on page 385](#)
 - [Understanding DHCP Option 82 on page 429](#)
 - [IPv6 Neighbor Discovery Inspection on page 509](#)
 - [Understanding ARP Spoofing and Inspection on page 449](#)
 - [Understanding IP Source Guard for Port Security on Switches on page 459](#)
 - [Understanding MAC Limiting and MAC Move Limiting on page 330](#)
 - [802.1X for Switches Overview](#)
 - [Understanding Proxy ARP](#)
 - [Understanding Storm Control on page 622](#)

Understanding How to Protect Access Ports from Common Attacks

Port security features can protect the Juniper Networks EX Series and QFX10000 Ethernet Switches against various types of attacks. Protection methods against some common attacks are:

- [Mitigation of Ethernet Switching Table Overflow Attacks on page 7](#)
- [Mitigation of Rogue DHCP Server Attacks on page 7](#)
- [Protection Against ARP Spoofing Attacks \(Does not apply to QFX10000 Series Switches\) on page 8](#)
- [Protection Against DHCP Snooping Database Alteration Attacks \(Does not apply to QFX10000 Series Switches\) on page 8](#)
- [Protection Against DHCP Starvation Attacks on page 8](#)

Mitigation of Ethernet Switching Table Overflow Attacks

In an overflow attack on the Ethernet switching table, an intruder sends so many requests from new MAC addresses that the table cannot learn all the addresses. When the switch can no longer use information in the table to forward traffic, it is forced to broadcast messages. Traffic flow on the switch is disrupted, and packets are sent to all hosts on the network. In addition to overloading the network with traffic, the attacker might also be able to sniff that broadcast traffic.

To mitigate such attacks, configure both a MAC limit for learned MAC addresses and some specific allowed MAC addresses. Use the MAC limiting feature to control the total number of MAC addresses that can be added to the Ethernet switching table for the specified interface or interfaces. By setting the MAC addresses that are explicitly allowed, you ensure that the addresses of network devices whose network access is critical are guaranteed to be included in the Ethernet switching table. See [“Example: Protecting against Ethernet Switching Table Overflow Attacks” on page 354](#).



NOTE: You can also configure learned MAC addresses to persist on each interface. Used in combination with a configured MAC limit, this persistent MAC learning helps prevent traffic loss after a restart or an interface-down event and also increases port security by limiting the MAC addresses allowed on the interface.

Mitigation of Rogue DHCP Server Attacks

If an attacker sets up a rogue DHCP server to impersonate a legitimate DHCP server on the LAN, the rogue server can start issuing leases to the network's DHCP clients. The information provided to the clients by this rogue server can disrupt their network access, causing DoS. The rogue server might also assign itself as the default gateway device for the network. The attacker can then sniff the network traffic and perpetrate a man-in-the-middle attack—that is, it misdirects traffic intended for a legitimate network device to a device of its choice.

To mitigate a rogue DHCP server attack, set the interface to which that rogue server is connected as untrusted. That action will block all ingress DHCP server messages from that interface. See [“Example: Protecting against Rogue DHCP Server Attacks” on page 351](#).



NOTE: The switch logs all DHCP server packets that are received on untrusted ports—for example:

```
5 untrusted DHCPOFFER received, interface ge-0/0/0.0[65], vlan v1[10] server
ip/mac 12.12.12.1/00:00:00:00:01:12 offer ip/client mac
12.12.12.253/00:AA:BB:CC:DD:01
```

You can use these messages to detect malicious DHCP servers on the network.



NOTE: For QFX Series switches, including QFX10000, if you attach a DHCP server to an access port, you must configure the port as trusted.

Protection Against ARP Spoofing Attacks (Does not apply to QFX10000 Series Switches)

In ARP spoofing, an attacker sends faked ARP messages on the network. The attacker associates its own MAC address with the IP address of a network device connected to the switch. Any traffic sent to that IP address is instead sent to the attacker. Now the attacker can create various types of mischief, including sniffing the packets that were meant for another host and perpetrating man-in-the-middle attacks. (In a man-in-the-middle attack, the attacker intercepts messages between two hosts, reads them, and perhaps alters them, all without the original hosts knowing that their communications have been compromised.)

To protect against ARP spoofing on your switch, enable both DHCP snooping and dynamic ARP inspection (DAI). DHCP snooping builds and maintains the DHCP snooping table. That table contains the MAC addresses, IP addresses, lease times, binding types, VLAN information, and interface information for the untrusted interfaces on the switch. DAI uses the information in the DHCP snooping table to validate ARP packets. Invalid ARP packets are blocked and, when they are blocked, a system log message is recorded that includes the type of ARP packet and the sender's IP address and MAC address.

See [“Example: Protecting Against ARP Spoofing Attacks”](#) on page 418.

Protection Against DHCP Snooping Database Alteration Attacks (Does not apply to QFX10000 Series Switches)

In an attack designed to alter the DHCP snooping database, an intruder introduces a DHCP client on one of the switch's untrusted access interfaces that has a MAC address identical to that of a client on another untrusted port. The intruder acquires the DHCP lease, which results in changes to the entries in the DHCP snooping table. Subsequently, what would have been valid ARP requests from the legitimate client are blocked.

To protect against this type of alteration of the DHCP snooping database, configure MAC addresses that are explicitly allowed on the interface. See [“Example: Protecting Against DHCP Snooping Database Attacks”](#) on page 415.

Protection Against DHCP Starvation Attacks

In a DHCP starvation attack, an attacker floods an Ethernet LAN with DHCP requests from spoofed (counterfeit) MAC addresses so that the switch's trusted DHCP servers cannot keep up with requests from legitimate DHCP clients on the switch. The address space of those servers is completely used up, so they can no longer assign IP addresses and lease times to clients. DHCP requests from those clients are either dropped—that is, the result is a denial of service (DoS)—or directed to a rogue DHCP server set up by the attacker to impersonate a legitimate DHCP server on the LAN.

To protect the switch from DHCP starvation attacks, use the MAC limiting feature. Specify the maximum number of MAC addresses that the switch can learn on the access interfaces

to which those clients connect. The switch's DHCP server or servers will then be able to supply the specified number of IP addresses and leases to those clients and no more. If a DHCP starvation attack occurs after the maximum number of IP addresses has been assigned, the attack will fail. See [“Example: Protecting against DHCP Starvation Attacks” on page 347](#).



NOTE: For additional protection on EX Series switches, you can configure learned MAC addresses on each interface to persist across restarts of the switch by enabling persistent MAC learning. This persistent MAC learning both helps to prevent traffic loss after a restart and ensures that even after a restart or an interface-down event, the persistent MAC addresses are re-entered into the forwarding database rather than the switch learning new MAC addresses.

- See Also**
- [Understanding DHCP Snooping \(non-ELS\) on page 393](#)
 - [Example: Setting Up DHCP Option 82 on page 433](#)
 - *OBSOLETE: Understanding Trusted DHCP Servers for Port Security*
 - [Understanding MAC Limiting and MAC Move Limiting on page 330](#)
 - [Understanding ARP Spoofing and Inspection on page 449](#)
 - [Configuring Port Security \(non-ELS\) on page 11](#)

Configuring Port Security (ELS)



NOTE: The features described are supported on EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see [“Configuring Port Security \(non-ELS\)” on page 11](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Ethernet LANs are vulnerable to attacks such as address spoofing and Layer 2 denial of service (DoS) on network devices. DHCP port security features help protect the access ports on the switch against the losses of information and productivity that can result from such attacks.

The following port security features are supported for DHCPv4:

- DHCP snooping
- Dynamic ARP inspection (DAI)
- IP source guard
- DHCP option 82

The following port security features are supported for DHCPv6:

- DHCPv6 snooping
- IPv6 Neighbor discovery inspection
- IPv6 source guard
- DHCPv6 option 37, option 18 and option 16

DHCP snooping and DHCPv6 snooping are disabled by default on any VLAN. No explicit CLI configuration is used to enable DHCP snooping or DHCPv6 snooping. When you configure any of the port security features for a VLAN at the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level, DHCP snooping and DHCPv6 snooping are automatically enabled on that VLAN.



NOTE: Starting in Junos OS Release 14.1X53-D47 and 15.1R6, you can enable DHCP snooping or DHCPv6 snooping on a VLAN without configuring other port security features by configuring the `dhcp-security` CLI statement at the **[edit vlans *vlan-name* forwarding-options]** hierarchy level.

DAI, IPv6 neighbor discovery inspection, IP source guard, IPv6 source guard, DHCP option 82 and DHCPv6 options are configured per VLAN. You must configure a VLAN before configuring these DHCP port security features. See *Configuring VLANs for EX Series Switches with ELS Support (CLI Procedure)*.

The DHCP port security features that you specify for the VLAN apply to all the interfaces included within that VLAN. However, you can assign different attributes to an access interface or a group of access interfaces within the VLAN. The access interface or interfaces must first be configured as a group using the `group` statement at the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level. A group must have at least one interface.



NOTE: Configuring a group of access interfaces on a VLAN at the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level automatically enables DHCP snooping for all interfaces in the VLAN.

Attributes that can be specified for access interfaces using the `group` statement are:

- Specifying that the interface have a static IP-MAC address (`static-ip` or `static-ipv6`)
- Specifying an access interface to act as a trusted interface to a DHCP server (`trusted`)
- Specifying an interface not to transmit DHCP option 82 (`no-option82`) or DHCPv6 options (`no-option37`)



NOTE: Trunk interfaces are trusted by default. However, you can override this default behavior and set a trunk interface as `untrusted`.

For additional details, see:

- [Enabling Dynamic ARP Inspection \(ELS\) on page 451](#)
- [IPv6 Neighbor Discovery Inspection on page 509](#)
- [Configuring IP Source Guard \(ELS\) on page 465](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\) on page 439](#)

You can override the general port security settings for the VLAN by configuring a group of access interfaces within that VLAN. For details, see:

- [Configuring Static DHCP IP Addresses for DHCP snooping \(ELS\) on page 404](#)
- [Enabling a Trusted DHCP Server \(ELS\) on page 372](#)

- See Also**
- [Port Security Features on page 3](#)
 - [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

Configuring Port Security (non-ELS)

Ethernet LANs are vulnerable to attacks such as address spoofing and Layer 2 denial of service (DoS) on network devices. Port security features such as DHCP snooping, DAI (dynamic ARP inspection), MAC limiting, MAC move limiting, and persistent MAC learning, as well as trusted DHCP server, help protect the access ports on the switch against the loss of information and productivity that such attacks can cause.

Depending on the particular feature, you can configure the port security feature either on:

- VLANs—A specific VLAN or all VLANs
- Interfaces—A specific interface or all interfaces



NOTE: If you configure one of the port security features on all VLANs or all interfaces, the switch software enables that port security feature on all VLANs and all interfaces that are not explicitly configured with other port security features.

However, if you do explicitly configure one of the port security features on a specific VLAN or on a specific interface, you must explicitly configure any additional port security features that you want to apply to that VLAN or interface. Otherwise, the switch software automatically applies the default values for the feature.

For example, if you disable DHCP snooping on all VLANs and decide to explicitly enable IP source guard only on a specific VLAN, you must also explicitly enable DHCP snooping on that specific VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

To configure port security features by using the CLI:

- [Enabling DHCP Snooping on page 12](#)
- [Enabling Dynamic ARP Inspection \(DAI\) on page 13](#)
- [Enabling IPv6 Neighbor Discovery Inspection on page 13](#)
- [Limiting Dynamic MAC Addresses on an Interface on page 13](#)
- [Enabling Persistent MAC Learning on an Interface on page 14](#)
- [Limiting MAC Address Movement on page 14](#)
- [Restricting a VoIP Client MAC Address in a VoIP VLAN on page 14](#)
- [Configuring Trusted DHCP Servers on an Interface on page 14](#)

Enabling DHCP Snooping

You can configure DHCP snooping to enable the device to monitor DHCP messages received, ensure that hosts use only the IP addresses that are assigned to them, and allow access only to authorized DHCP servers.

To enable DHCP snooping:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name examine-dhcp
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all examine-dhcp
```

To enable DHCPv6 snooping:

- On a specific VLAN:


```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name examine-dhcpv6
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all examine-dhcpv6
```

Enabling Dynamic ARP Inspection (DAI)

You can enable DAI to protect against ARP snooping. To enable DAI:

- On a single VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name arp-inspection
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all arp-inspection
```

Enabling IPv6 Neighbor Discovery Inspection

You can enable neighbor discovery inspection to protect against IPv6 address spoofing.

- To enable neighbor discovery on a single VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name neighbor-discovery-inspection
```

- To enable neighbor discovery on all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all neighbor-discovery-inspection
```

Limiting Dynamic MAC Addresses on an Interface

Limit the number of dynamic MAC addresses allowed on an interface and specify the action to take if the limit is exceeded:

- On a single interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name mac-limit limit action action
```

- On all interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all mac-limit limit action action
```

Enabling Persistent MAC Learning on an Interface

You can configure learned MAC addresses to persist on an interface across restarts of the switch:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name persistent-learning
```

Limiting MAC Address Movement

You can limit the number of times a MAC address can move from its original interface in 1 second:

- On a single VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name mac-move-limit limit action action
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all mac-move-limit limit action action
```

Restricting a VoIP Client MAC Address in a VoIP VLAN

To restrict a VoIP client MAC address from being learned in a configured VoIP VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name voip-mac-exclusive
```

Any MAC address learned on that interface for the VoIP VLAN is not learned on a data VLAN with that same interface. If a MAC address has been learned on a data VLAN interface and then the MAC address is learned on a VoIP VLAN with that same interface, the MAC address is removed from the data VLAN interface.

Configuring Trusted DHCP Servers on an Interface

Configure a trusted DHCP server on an interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name dhcp-trusted
```

- See Also**
- [Configuring Autorecovery for Port Security Events on page 635](#)
 - [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks on page 406](#)
 - [Monitoring Port Security](#)
 - [Port Security Features on page 3](#)
 - [secure-access-port on page 979](#)

Example: Configuring Port Security (non-ELS)

You can configure DHCP snooping, dynamic ARP inspection (DAI), MAC limiting, persistent MAC learning, and MAC move limiting on the untrusted ports of switches to protect the switches and the Ethernet LAN against address spoofing and Layer 2 denial-of-service (DoS) attacks. You can also configure a trusted DHCP server and specific (allowed) MAC addresses for the switch interfaces.



NOTE: The switches used in this example do not support the ELS configuration style. For information on configuring port security on ELS switches, see [“Configuring Port Security \(ELS\)” on page 9](#).

This example describes how to configure basic port security features on a switch:

- [Requirements on page 15](#)
- [Overview and Topology on page 15](#)
- [Configuration on page 17](#)
- [Verification on page 19](#)

Requirements

This example uses the following hardware and software components:

- One EX Series or QFX Series.
- Junos OS Release 11.4 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure basic port security features, be sure you have:

- Connected the DHCP server to the switch.
- Configured a VLAN on the switch. See the task for your platform:
 - [Configuring VLANs for EX Series Switches](#)



NOTE: In this example, the DHCP server and its clients are all members of a single VLAN on the switch.

Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. To protect the devices from such attacks, you can configure:

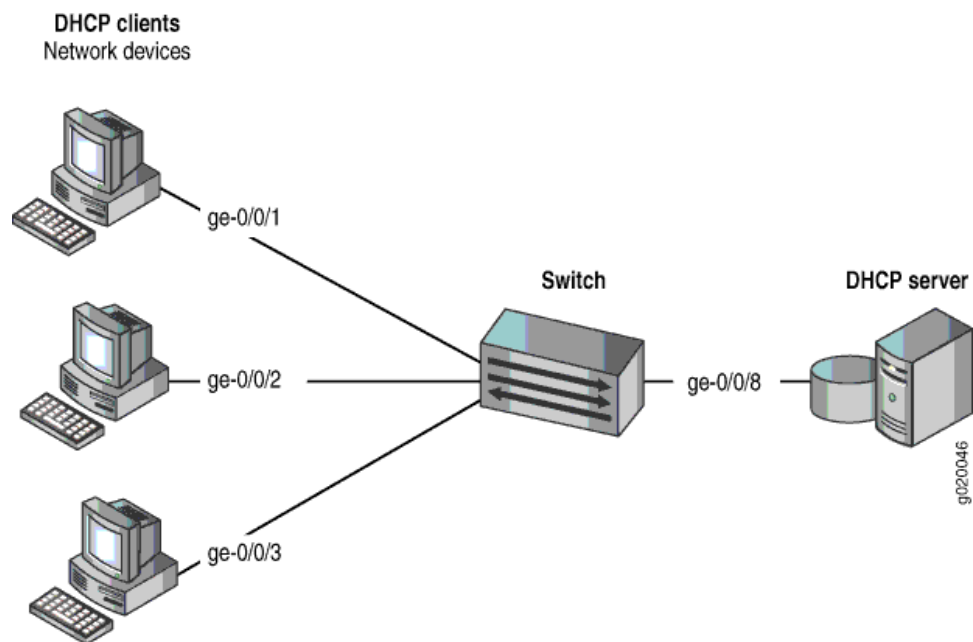
- DHCP snooping to validate DHCP server messages
- DAI to protect against MAC spoofing

- MAC limiting to constrain the number of MAC addresses the switch adds to its MAC address cache
- MAC move limiting to help prevent MAC spoofing
- Persistent MAC learning (sticky MAC) to constrain the MAC addresses that can be learned on an interface to the first ones learned, even after a reboot of the switch
- Trusted DHCP server configured on a trusted port to protect against rogue DHCP servers sending leases

This example shows how to configure these security features on a switch connected to a DHCP server.

The setup for this example includes the VLAN **employee-vlan** on the switch. [Figure 1 on page 16](#) illustrates the topology for this example.

Figure 1: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 3 on page 16](#).

Table 3: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX Series or QFX series switch
VLAN name and ID	employee-vlan , tag 20
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is subnet's broadcast address
Interfaces in employee-vlan	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8

Table 3: Components of the Port Security Topology (continued)

Properties	Settings
Interface for DHCP server	ge-0/0/8

In this example, the switch is initially configured with the default port security setup. In the default switch configuration:

- Secure port access is activated on the switch.
- DHCP snooping and DAI are disabled on all VLANs.
- All access ports are untrusted, and all trunk ports are trusted for DHCP snooping.

In the configuration tasks for this example, you set the DHCP server as trusted; you enable DHCP snooping, DAI, and MAC move limiting on a VLAN; you set a value for a MAC limit on some interfaces; you configure some specific (allowed) MAC addresses on an interface; and you configure persistent MAC learning on an interface.

Configuration

To configure basic port security on a switch whose DHCP server and client ports are in a single VLAN:

CLI Quick Configuration

To quickly configure basic port security on the switch, copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/1 mac-limit 4
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88
set interface ge-0/0/2 mac-limit 4
set interface ge-0/0/1 persistent-learning
set interface ge-0/0/8 dhcp-trusted
set vlan employee-vlan arp-inspection
set vlan employee-vlan examine-dhcp
set vlan employee-vlan mac-move-limit 5
```

Step-by-Step Procedure

Configure basic port security on the switch:

1. Enable DHCP snooping on the VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan examine-dhcp
```

2. Specify the interface (port) from which DHCP responses are allowed:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/8 dhcp-trusted
```

3. Enable dynamic ARP inspection (DAI) on the VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan arp-inspection
```

4. Configure a MAC limit of 4 and use the default action, **drop**. (Packets are dropped, and the MAC address is not added to the Ethernet switching table if the MAC limit is exceeded on the interfaces):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 mac-limit 4
user@switch# set interface ge-0/0/2 mac-limit 4
```

5. Allow learned MAC addresses for a particular interface to persist across restarts of the switch and interface-down events by enabling persistent MAC learning:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 persistent-learning
```

6. Configure a MAC move limit of 5 and use the default action, **drop**. (Packets are dropped, and the MAC address is not added to the Ethernet switching table if a MAC address has exceeded the MAC move limit):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan mac-move-limit 5
```

7. Configure allowed MAC addresses:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88
```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/1.0 {
  mac-limit 4;
  persistent-learning;
}
interface ge-0/0/2.0 {
  allowed-mac [ 00:05:85:3a:82:80 00:05:85:3a:82:81 00:05:85:3a:82:83
    00:05:85:3a:82:85 00:05:85:3a:82:88 ];
  mac-limit 4;
}
interface ge-0/0/8.0 {
  dhcp-trusted;
}
vlan employee-vlan {
  arp-inspection
  examine-dhcp;
```

```
mac-move-limit 5;
}
```

Verification

To confirm that the configuration is working properly:

- [Verifying That DHCP Snooping Is Working Correctly on the Switch on page 19](#)
- [Verifying That DAI Is Working Correctly on the Switch on page 19](#)
- [Verifying That MAC Limiting, MAC Move Limiting, and Persistent MAC Learning Are Working Correctly on the Switch on page 20](#)
- [Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 21](#)

Verifying That DHCP Snooping Is Working Correctly on the Switch

Purpose Verify that DHCP snooping is working on the switch.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp snooping binding
```

DHCP Snooping Information:

MAC Address	IP Address	Lease	Type	VLAN	Interface
00:05:85:3A:82:77	192.0.2.17	600	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:79	192.0.2.18	653	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:80	192.0.2.19	720	dynamic	employee-vlan	ge-0/0/2.0
00:05:85:3A:82:81	192.0.2.20	932	dynamic	employee-vlan	ge-0/0/2.0
00:05:85:3A:82:83	192.0.2.21	1230	dynamic	employee-vlan	ge-0/0/2.0
00:05:85:27:32:88	192.0.2.22	3200	dynamic	employee-vlan	ge-0/0/2.0

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

If the DHCP server had been configured as untrusted, no entries would be added to the DHCP snooping database, and nothing would be shown in the output of the **show dhcp snooping binding** command.

Verifying That DAI Is Working Correctly on the Switch

Purpose Verify that DAI is working on the switch.

Action Send some ARP requests from network devices connected to the switch.

Display the DAI information:

```
user@switch> show arp inspection statistics
```

ARP inspection statistics:

Interface	Packets received	ARP inspection pass	ARP inspection failed
-----	-----	-----	-----
ge-0/0/1.0	7	5	2
ge-0/0/2.0	10	10	0
ge-0/0/3.0	12	12	0

Meaning The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

Verifying That MAC Limiting, MAC Move Limiting, and Persistent MAC Learning Are Working Correctly on the Switch

Purpose Verify that MAC limiting, MAC move limiting, and persistent MAC learning are working on the switch.

Action Suppose that two packets have been sent from hosts on **ge-0/0/1** and five packets from hosts on **ge-0/0/2**, with both interfaces set to a MAC limit of 4 with the default action **drop** and **ge-0/0/1** enabled for persistent MAC learning.

Display the MAC addresses learned:

```
user@switch> show ethernet-switching table
```

Ethernet-switching table: 7 entries, 4 learned, 2 persistent entries				
VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	-	All-members
employee-vlan	00:05:85:3A:82:77	Persistent	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:79	Persistent	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0

Now suppose packets have been sent from two of the hosts on **ge-0/0/2** after they have been moved to other interfaces more than five times in 1 second, with **employee-vlan** set to a MAC move limit of 5 with the default action **drop**.

Display the MAC addresses in the table:

```
user@switch> show ethernet-switching table
```

Ethernet-switching table: 7 entries, 2 learned, 2 persistent entries				
VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	-	All-members
employee-vlan	00:05:85:3A:82:77	Persistent	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:79	Persistent	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

Meaning The first sample output shows that with a MAC limit of 4 for each interface, the fifth MAC address on **ge-0/0/2** was not learned because it exceeded the MAC limit. The second sample output shows that MAC addresses for three of the hosts on **ge-0/0/2** were not learned, because the hosts had been moved back more than five times in 1 second.

Interface **ge-0/0/1.0** was enabled for persistent MAC learning, so the MAC addresses associated with this interface are of the type **persistent**.

Verifying That Allowed MAC Addresses Are Working Correctly on the Switch

Purpose Verify that allowed MAC addresses are working on the switch.

Action Display the MAC cache information after five allowed MAC addresses have been configured on interface **ge-0/0/2**:

```
user@switch> show ethernet-switching table
```

Ethernet-switching table: 5 entries, 4 learned

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

Meaning Because the MAC limit value for this interface has been set to 4, only four of the five configured allowed addresses are learned.

See Also

- [Example: Protecting against Rogue DHCP Server Attacks on page 351](#)
- [Example: Protecting Against ARP Spoofing Attacks on page 418](#)
- [Example: Protecting Against DHCP Snooping Database Attacks on page 415](#)
- [Configuring Port Security \(non-ELS\) on page 11](#)

PART 2

IPSec

- [Understanding IPsec and Security Associations on page 25](#)
- [IPsec Configurations and Examples on page 31](#)
- [Configuring IPsec Security Associations on page 53](#)
- [Using Digital Certificates for IPsec on page 73](#)
- [Additional IPsec Options on page 79](#)
- [Configuring IPsec Dynamic Endpoints on page 85](#)
- [Additional ES and AS PIC Configuration Examples on page 93](#)

CHAPTER 2

Understanding IPsec and Security Associations

- [IPSec Terms and Acronyms on page 25](#)
- [Security Associations Overview on page 27](#)
- [IKE Key Management Protocol Overview on page 28](#)
- [IPsec Requirements for Junos-FIPS on page 30](#)

IPSec Terms and Acronyms

A

Adaptive Services PIC	A next-generation Physical Interface Card (PIC) that provides IPsec services and other services, such as Network Address Translation (NAT) and stateful firewall, on M Series and T Series platforms.
Advanced Encryption Standard (AES)	A next-generation encryption method that is based on the Rijndael algorithm and uses a 128-bit block, three different key sizes (128, 192, and 256 bits), and multiple rounds of processing to encrypt data.
authentication header (AH)	A component of the IPsec protocol used to verify that the contents of a packet have not changed (data integrity), and to validate the identity of the sender (data source authentication). For more information about AH, see RFC 2402.

C

certificate authority (CA)	A trusted third-party organization that generates, enrolls, validates, and revokes digital certificates. The CA guarantees the identity of a user and issues public and private keys for message encryption and decryption.
certificate revocation list (CRL)	A list of digital certificates that have been invalidated before their expiration date, including the reasons for their revocation and the names of the entities that have issued them. A CRL prevents usage of digital certificates and signatures that have been compromised.
cipher block chaining (CBC)	A cryptographic method that encrypts blocks of ciphertext by using the encryption result of one block to encrypt the next block. Upon decryption, the validity of each block of ciphertext depends on the validity of all the preceding ciphertext blocks. For more information on how to use CBC with DES and ESP to provide confidentiality, see RFC 2405.

D

Data Encryption Standard (DES)	An encryption algorithm that encrypts and decrypts packet data by processing the data with a single shared key. DES operates in increments of 64-bit blocks and provides 56-bit encryption.
digital certificate	Electronic file that uses private and public key technology to verify the identity of a certificate creator and distribute keys to peers.

E

Encapsulating Security Payload (ESP)	A component of the IPsec protocol used to encrypt data in an IPv4 or IPv6 packet, provide data integrity, and ensure data source authentication. For more information about ESP, see RFC 2406.
ES PIC	A PIC that provides first-generation encryption services and software support for IPsec on M Series and T Series platforms.

H

Hashed Message Authentication Code (HMAC)	A mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, such as MD5 or SHA-1, in combination with a secret shared key. For more information on HMAC, see RFC 2104.
--	--

I

Internet Key Exchange (IKE)	Establishes shared security parameters for any hosts or routers using IPsec. IKE establishes the SAs for IPsec. For more information about IKE, see RFC 2407.
------------------------------------	---

M

Message Digest 5 (MD5)	An authentication algorithm that takes a data message of arbitrary length and produces a 128-bit message digest. For more information, see RFC 1321.
-------------------------------	--

P

Perfect Forward Secrecy (PFS)	Provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.
public key infrastructure (PKI)	A trust hierarchy that enables users of a public network to securely and privately exchange data through the use of public and private cryptographic key pairs that are obtained and shared with peers through a trusted authority.

R

registration authority (RA)	A trusted third-party organization that acts on behalf of a CA to guarantee the identity of a user.
Routing Engine	A PCI-based architectural portion of a Junos OS-based router that handles the routing protocol process, the interface process, some of the chassis components, system management, and user access.

S

Secure Hash Algorithm 1 (SHA-1)	An authentication algorithm that takes a data message of less than 264 bits in length and produces a 160-bit message digest. For more information on SHA-1, see RFC 3174.
Secure Hash Algorithm 2 (SHA-2)	A successor to the SHA-1 authentication algorithm that includes a group of SHA-1 variants (SHA-224, SHA-256, SHA-384, and SHA-512). SHA-2 algorithms use larger hash sizes and are designed to work with enhanced encryption algorithms such as AES.
security association (SA)	Specifications that must be agreed upon between two network devices before IKE or IPsec are allowed to function. SAs primarily specify protocol, authentication, and encryption options.
Security Association Database (SADB)	A database where all SAs are stored, monitored, and processed by IPsec.
Security Parameter Index (SPI)	An identifier that is used to uniquely identify an SA at a network host or router.
Security Policy Database (SPD)	A database that works with the SADB to ensure maximum packet security. For inbound packets, IPsec checks the SPD to verify if the incoming packet matches the security configured for a particular policy. For outbound packets, IPsec checks the SPD to see if the packet needs to be secured.
Simple Certificate Enrollment Protocol (SCEP)	A protocol that supports CA and registration authority (RA) public key distribution, certificate enrollment, certificate revocation, certificate queries, and certificate revocation list (CRL) queries.

T

Triple Data Encryption Standard (3DES)	An enhanced DES algorithm that provides 168-bit encryption by processing data three times with three different keys.
---	--

Security Associations Overview

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

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

- Set up user-level tunnels or SAs, including tunnel attribute negotiations and key management. These tunnels can also be refreshed and terminated on top of the same secure channel.

The Junos OS implementation of IPsec supports two modes of security (transport mode and tunnel mode).

**Related
Documentation**

- *[IKE Key Management Protocol Overview](#)*
- *[IPsec Requirements for Junos-FIPS](#)*
- *[\[edit security\] Hierarchy Level](#)*

IKE Key Management Protocol Overview

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

IKE does the following:

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

IKE occurs over two phases. In the first phase, it negotiates security attributes and establishes shared secrets to form the bidirectional IKE SA. In the second phase, inbound and outbound IPsec SAs are established. The IKE SA secures the exchanges in the second phase. IKE also generates keying material, provides Perfect Forward Secrecy, and exchanges identities.



NOTE: Starting in Junos OS Release 14.2, when you perform an SNMP walk of the `jnxIkeTunnelEntry` object in the `jnxIkeTunnelTable` table, the **Request failed: OID not increasing** error message might be generated. This problem occurs only when simultaneous Internet Key Exchange security associations (IKE SAs) are created, which occurs when both ends of the SA initiate IKE SA negotiations at the same time. When an SNMP MIB walk is performed to display IKE SAs, the `snmpwalk` tool expects the object identifiers (OIDs) to be in increasing order. However, in the case of simultaneous IKE SAs, the OIDs in the SNMP table might not be in increasing order. This behavior occurs because the tunnel IDs, which are part of the OIDs, are allocated based on the initiator of the IKE SA, which can be on either side of the IKE tunnel.

The following is an example of an SNMP MIB walk that is performed on IKE simultaneous SAs:

```
jnxIkeTunnelLocalRole."ipsec_ss_cust554".ipv4."192.0.2.41".47885 = INTEGER:
responder(2)    >>> This is Initiator SA
jnxIkeTunnelLocalRole."ipsec_ss_cust554".ipv4."192.0.2.41".47392 = INTEGER:
initiator(1)    >>> This is Responder's SA
```

The OID comparison fails when the SNMP walk is tunnel ID (47885 and 47392). It cannot be ensured when an SNMP walk is performed that the tunnel IDs are in increasing order because tunnels might be initiated from either side.

To work around this problem, the SNMP MIB walk contains an option, `-Cc`, to disable check for increasing OIDs. The following is an example of the MIB walk performed on the `jnxIkeTunnelEntry` table with the `-Cc` option:

```
snmpwalk -Os -Cc -c public -v 1 vira jnxIkeTunnelEntry
```

Release History Table

Release	Description
14.2	Starting in Junos OS Release 14.2, when you perform an SNMP walk of the <code>jnxIkeTunnelEntry</code> object in the <code>jnxIkeTunnelTable</code> table, the Request failed: OID not increasing error message might be generated.

Related Documentation

- [Security Associations Overview](#)
- [IPsec Requirements for Junos-FIPS](#)
- [\[edit security\] Hierarchy Level](#)

IPsec Requirements for Junos-FIPS

In a Junos-FIPS environment, hardware configurations with two Routing Engines must be configured to use IPsec and a private routing instance for all communications between the Routing Engines. IPsec communication between the Routing Engines and AS II FIPS PICs is also required.

- Related Documentation**
- *Security Associations Overview*
 - *IKE Key Management Protocol Overview*
 - *[edit security] Hierarchy Level*

CHAPTER 3

IPsec Configurations and Examples

- [Considering General IPsec Issues on page 31](#)
- [IPsec Configuration for an ES PIC Overview on page 35](#)
- [Configuring Security Associations for IPsec on an ES PIC on page 37](#)
- [Configuring IPsec Security Associations on page 39](#)
- [Configuring an IKE Policy on page 44](#)
- [Configuring an IPsec Proposal for an ES PIC on page 47](#)
- [Configuring an IPsec Policy on page 49](#)

Considering General IPsec Issues

Before you configure IPsec, it is helpful to understand some general guidelines.

- **IPv4 and IPv6 traffic and tunnels**—You can configure IPsec tunnels to carry traffic in the following ways: IPv4 traffic traveling over IPv4 IPsec tunnels, IPv6 traffic traveling over IPv4 IPsec tunnels, IPv4 traffic traveling over IPv6 IPsec tunnels, and IPv6 traffic traveling over IPv6 IPsec tunnels.
- **Configuration syntax differences between the AS and MultiServices PICs and the ES PIC**—There are slight differences in the configuration statements and operational mode commands that are used with the PICs that support IPsec. As a result, the syntax for the AS and MultiServices PICs cannot be used interchangeably with the syntax for the ES PIC. However, the syntax for one type of PIC can be converted to its equivalent syntax on the other PIC for interoperability. The syntax differences are highlighted in [Table 4 on page 31](#).
- **Configuring keys for authentication and encryption**—When preshared keys are required for authentication or encryption, you must use the guidelines shown in [Table 5 on page 33](#) to implement the correct key size.
- **Rejection of weak and semiweak keys**—The DES and 3DES encryption algorithms will reject weak and semiweak keys. As a result, do not create and use keys that contain the patterns listed in [Table 6 on page 34](#).

Table 4: Comparison of IPsec Configuration Statements and

Table 4: Comparison of IPsec Configuration Statements and Operational Mode Commands for the AS and MultiServices PICs and ES PIC (continued)
Operational Mode Commands for the AS and MultiServices PICs and ES PIC

AS and MultiServices PICs Statements and Commands	ES PIC Statements and Commands
Configuration Mode Statements	
[edit service-set <i>name</i>]	—
[edit services ipsec-vpn ike] <ul style="list-style-type: none"> • policy {...} • proposal {...} 	[edit security ike] <ul style="list-style-type: none"> • policy {...} • proposal {...}
[edit services ipsec-vpn ipsec] <ul style="list-style-type: none"> • policy {...} • proposal {...} 	[edit security ipsec] <ul style="list-style-type: none"> • policy {...} • proposal {...}
[edit services ipsec-vpn rule <i>rule-name</i>] <ul style="list-style-type: none"> • remote-gateway <i>address</i> 	[edit interface es- <i>fpc</i> / <i>pic</i> / <i>port</i>] <ul style="list-style-type: none"> • tunnel destination <i>address</i>
[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i>] <ul style="list-style-type: none"> • from <i>match-conditions</i> {...} then dynamic {...} • from <i>match-conditions</i> {...} then manual {...} 	[edit security ipsec] <ul style="list-style-type: none"> • security-association <i>name</i> dynamic {...} • security-association <i>name</i> manual {...}
[edit services ipsec-vpn rule-set]	—
[edit services service-set ipsec-vpn] <ul style="list-style-type: none"> • local-gateway <i>address</i> 	[edit interface es- <i>fpc</i> / <i>pic</i> / <i>port</i>] <ul style="list-style-type: none"> • tunnel source <i>address</i>
Operational Mode Commands	
clear security pki ca-certificate	—
clear security pki certificate-request	—
clear security pki local-certificate	—
clear services ipsec-vpn certificates	—
request security pki ca-certificate enroll	request security certificate (unsigned)
request security pki ca-certificate load	request system certificate add
request security pki generate-certificate-request	—

Table 4: Comparison of IPsec Configuration Statements and Operational Mode Commands for the AS and MultiServices PICs and ES PIC (continued)

AS and MultiServices PICs Statements and Commands	ES PIC Statements and Commands
<code>request security pki generate-key-pair</code>	<code>request security key-pair</code>
<code>request security pki local-certificate enroll</code>	<code>request security certificate (signed)</code>
<code>request security pki local-certificate load</code>	<code>request system certificate add</code>
<code>show security pki ca-certificate</code>	<code>show system certificate</code>
<code>show security pki certificate-request</code>	—
<code>show security pki crl</code>	—
<code>show security pki local-certificate</code>	<code>show system certificate</code>
<code>show services ipsec-vpn certificates</code>	<code>show ipsec certificates</code>
<code>show services ipsec-vpn ike security-associations</code>	<code>show ike security-associations</code>
<code>show services ipsec-vpn ipsec security-associations</code>	<code>show ipsec security-associations</code>

Table 5: Authentication and Encryption Key Lengths

	Number of Hexadecimal Characters	Number of ASCII Characters
Authentication		
HMAC-MD5-96	32	16
HMAC-SHA1-96	40	20
Encryption		
AES-128-CBC	16	32
AES-192-CBC	24	48
AES-256-CBC	32	64
DES-CBC	16	8
3DES-CBC	48	24

Table 6: Weak and Semiweak Keys

Weak Keys			
0101	0101	0101	0101
1F1F	1F1F	1F1F	1F1F
E0E0	E0E0	E0E0	E0E0
FEFE	FEFE	FEFE	FEFE
Semiweak Keys			
01FE	01FE	01FE	01FE
1FE0	1FE0	0EF1	0EF1
01E0	01E0	01F1	01F1
1FFE	1FFE	0EFE	0EFE
011F	011F	010E	010E
E0FE	E0FE	F1FE	F1FE
FE01	FE01	FE01	FE01
E01F	E01F	F10E	F10E
E001	E001	F101	F101
FEF1	FEF1	FE0E	FE0E
1F01	1F01	0E01	0E01
FEE0	FEE0	FEF1	FEF1

Keep in mind the following limitations of IPsec services on the AS PIC:

- The AS PIC does not transport packets containing IPv4 options across IPsec tunnels. If you try to send packets containing IP options across an IPsec tunnel, the packets are dropped. Also, if you issue a **ping** command with the **record-route** option across an IPsec tunnel, the **ping** command fails.
- The AS PIC does not transport packets containing the following IPv6 options across IPsec tunnels: hop-by-hop, destination (Type 1 and 2), and routing. If you try to send packets containing these IPv6 options across an IPsec tunnel, the packets are dropped.
- Destination class usage is not supported with IPsec services on the AS PIC.

IPsec Configuration for an ES PIC Overview

- [IPsec Configuration for an ES PIC Overview on page 35](#)
- [Configuring Manual SAs on an ES PIC on page 35](#)
- [Configuring IKE Requirements on an ES PIC on page 36](#)
- [Configuring a Digital Certificate for IKE on an ES PIC on page 36](#)

IPsec Configuration for an ES PIC Overview

IP Security (IPsec) provides a secure way to authenticate senders and encrypt IPv4 and IPv6 traffic between network devices, such as routers and hosts. The following sections show how to configure IPsec for an ES PIC.

The key management process (**kmd**) provides IPsec authentication services for ES PICs. The key management process starts only when IPsec is configured on the router.

- See Also**
- [Configuring Manual SAs on an ES PIC on page 35](#)
 - [Configuring a Digital Certificate for IKE on an ES PIC on page 36](#)
 - [Configuring Security Associations for IPsec on an ES PIC on page 37](#)
 - [Configuring an IKE Proposal for Dynamic SAs](#)
 - [Example: Configuring an IKE Proposal](#)

Configuring Manual SAs on an ES PIC

To define a manual security association (SA) configuration for an ES PIC, include at least the following statements at the **[edit security ipsec]** hierarchy level:

```
[edit security ipsec]
security-association sa-name {
  manual {
    direction (inbound | outbound | bidirectional) {
      authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
      }
      protocol (ah | esp | bundle);
      spi spi-value;
    }
  }
}
```

- See Also**
- [IPsec Configuration for an ES PIC Overview on page 35](#)

Configuring IKE Requirements on an ES PIC

To define an IKE configuration for an ES PIC, include at least the following statements at the `[edit security]` hierarchy level:

```
[edit security ike]
proposal ike-proposal-name {
  authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
  dh-group (group1 | group2);
  encryption-algorithm (3des-cbd | des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc);
}
policy ike-peer-address {
  proposals [ ike-proposal-names ];
  pre-shared-key (ascii-text key | hexadecimal key);
}
```

See Also • [IPsec Configuration for an ES PIC Overview on page 35](#)

Configuring a Digital Certificate for IKE on an ES PIC

To define a digital certificate configuration for IKE for an encryption interface on M Series and T Series routers, include at least the following statements at the `[edit security certificates]` and `[edit security ike]` hierarchy levels:

```
[edit security]
certificates {
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl filename;
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
}
ike {
  policy ike-peer-address {
    local-certificate certificate-filename;
    local-key-pair private-public-key-file;
    proposal [ ike-proposal-names ];
  }
  proposal ike-proposal-name {
    authentication-method rsa-signatures;
  }
}
```

See Also • [IPsec Configuration for an ES PIC Overview on page 35](#)

Configuring Security Associations for IPsec on an ES PIC

To use IPsec security services, you create an SA between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. You can configure two types of SAs:

- **Manual**—Requires no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place. For information about how to configure a manual SA, see [“Configuring Manual IPsec Security Associations for an ES PIC” on page 39](#).
- **Dynamic**—Specify proposals to be negotiated with the tunnel peer. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more **proposal** statements, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer. For information about how to configure a dynamic SA, see [“Associating the Configured Security Association with a Logical Interface” on page 184](#).



NOTE: The Junos OS does not perform a commit check when an SA name referenced in the Border Gateway Protocol (BGP) protocol section is not configured at the `[edit security ipsec]` hierarchy level.

We recommend that you configure no more than 512 dynamic security associations per ES Physical Interface Card (PIC).

To configure an SA for IPsec for an ES PIC, include the **security-association** statement at the `[edit security ipsec]` hierarchy level:

```
[edit security ipsec]
security-association sa-name;
```



NOTE: You configure a dynamic SA for the AS and MultiServices PICs at the `[edit services ipsec-vpn rule rule-name term term-name then dynamic]`, `[edit services ipsec-vpn ike]`, and `[edit services ipsec-vpn ipsec]` hierarchy levels.

For more information, see the “IPsec Services Configuration Guidelines” chapter of the *Junos OS Services Interfaces Library for Routing Devices*.

Tasks to configure SAs for IPsec for an ES PIC are:

1. [Configuring the Description for an SA on page 38](#)
2. [Configuring IPsec Transport Mode on page 38](#)
3. [Configuring IPsec Tunnel Mode on page 38](#)

Configuring the Description for an SA

To specify a description for an IPsec SA, include the **description** statement at the **edit security ipsec security-association sa-name** hierarchy level:

```
[edit security ipsec security-association sa-name]  
description description;
```

Configuring IPsec Transport Mode

In transport mode, the data portion of the IP packet is encrypted, but the IP header is not. Transport mode can be used only when the communication endpoint and cryptographic endpoint are the same. Virtual private network (VPN) gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications. You configure manual SAs, and you must configure static values on both ends of the SA.



NOTE: When you use transport mode, the Junos OS supports both BGP and OSPFv3 for manual SAs.

To configure IPsec security for transport mode, include the **mode** statement with the **transport** option at the **edit security ipsec security-association sa-name** hierarchy level:

```
[edit security ipsec security-association sa-name]  
mode transport;
```

To apply tunnel mode, you configure manual SAs in transport mode and then reference the SA by name at the **[edit protocols bgp]** hierarchy level to protect a session with a given peer.



NOTE: You can configure BGP to establish a peer relationship over encrypted tunnels.

Configuring IPsec Tunnel Mode

You use tunnel mode when you use preshared keys with IKE to authenticate peers, or digital certificates with IKE to authenticate peers.

When you use preshared keys, you manually configure a preshared key, which must match that of its peer. With digital certificates, each router is dynamically or manually enrolled with a certificate authority (CA). When a tunnel is established, the public keys used for IPsec are dynamically obtained through IKE and validated against the CA certificate. This avoids the manual configuration of keys on routers within the topology. Adding a new router to the topology does not require any security configuration changes to existing routers.

To configure the IPsec in tunnel mode, include the **mode** statement with the **tunnel** option at the **edit security ipsec security-association sa-name** hierarchy level:

```
[edit security ipsec security-association sa-name]
mode tunnel;
```



NOTE: The Junos OS supports both BGP and OSPFv3 in transport mode.

To enable tunnel mode, follow the steps in these sections:

- [Configuring an IKE Proposal for Dynamic SAs](#)
- [Associating the Configured Security Association with a Logical Interface on page 184](#)
- [IPsec Tunnel Traffic Configuration Overview on page 197](#)

Configuring IPsec Security Associations

- [Configuring Manual IPsec Security Associations for an ES PIC on page 39](#)
- [Configuring Dynamic IPsec Security Associations on page 43](#)

Configuring Manual IPsec Security Associations for an ES PIC

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

Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. As a result, peers can communicate only when they all share the same configured options.

To configure the manual IPsec SA for an ES PIC, include the **manual** statement at the **edit security ipsec security-association sa-name** hierarchy level:

```
[edit security ipsec security-association sa-name]
manual {
  direction (inbound | outbound | bi-directional) {
    authentication {
      algorithm (hmac-md5-96 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    auxiliary-spi auxiliary-spi-value;
    encryption {
      algorithm (des-cbc | 3des-cbc);
      key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
  }
}
```

```
}
```

Tasks to configure a manual SA are:

1. [Configuring the Processing Direction on page 40](#)
2. [Configuring the Protocol for a Manual SA on page 41](#)
3. [Configuring the Security Parameter Index on page 41](#)
4. [Configuring the Auxiliary Security Parameter Index on page 42](#)
5. [Configuring the Authentication Algorithm and Key on page 42](#)
6. [Configuring the Encryption Algorithm and Key on page 42](#)

Configuring the Processing Direction

The **direction** statement sets inbound and outbound IPsec processing. If you want to define different algorithms, keys, or security parameter index (SPI) values for each direction, you configure the **inbound** and **outbound** options. If you want the same attributes in both directions, use the **bidirectional** option.

To configure the direction of IPsec processing, include the **direction** statement and specify the direction at the **[edit security ipsec security-association sa-name manual]** hierarchy level:

```
[edit security ipsec security-association sa-name manual]
direction (inbound | outbound | bidirectional);
```

The following example shows how to define different algorithms, keys, and security parameter index values for inbound and outbound processing directions:

```
[edit security ipsec security-association sa-name]
manual {
  direction inbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 23456789012345678901234;
    }
    protocol esp;
    spi 16384;
  }
  direction outbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 12345678901234567890abcd;
    }
    protocol esp;
    spi 24576;
  }
}
```

The following example shows how to define the same algorithms, keys, and security parameter index values for bidirectional processing:

```
[edit security ipsec security-association sa-name manual]
direction bidirectional {
  authentication {
    algorithm hmac-md5-96;
    key ascii-text 123456789012abcd;
  }
  protocol ah;
  spi 20001;
}
```

Configuring the Protocol for a Manual SA

IPsec uses two protocols to protect IP traffic: Encapsulating Security Payload (ESP) and authentication header (AH). For transport mode SAs, both ESP and AH are supported. The AH protocol is used for strong authentication. The **bundle** option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.



NOTE: The AH protocol is supported only on M Series routers.

To configure the IPsec protocol on an ES PIC, include the **protocol** statement at the **edit security ipsec security-association sa-name manual direction (inbound | outbound | bidirectional)]** hierarchy level and specify the **ah**, **bundle**, or **esp** option:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bi-directional)]
protocol (ah | bundle | esp);
```

Configuring the Security Parameter Index

An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets.



NOTE: Each manual SA must have a unique SPI and protocol combination.

Use the auxiliary SPI when you configure the protocol statement to use the **bundle** option.

To configure the SPI on an ES PIC, include the **spi** statement and specify a value (256 through 16,639) at the **[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]** hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bidirectional)]
spi spi-value;
```

Configuring the Auxiliary Security Parameter Index

When you configure the **protocol statement to use the bundle** option, the Junos OS uses the auxiliary SPI for the ESP and the SPI for the AH.



NOTE: Each manual SA must have a unique SPI and protocol combination.

To configure the auxiliary SPI, include the **auxiliary-spi** statement at the **[edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]** hierarchy level and set the value to an integer between 256 and 16,639:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bidirectional)]
auxiliary-spi auxiliary-spi-value;
```

Configuring the Authentication Algorithm and Key

To configure an authentication algorithm and key, include the **authentication** statement at the **[edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]** hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound |
bidirectional)]
authentication {
  algorithm (hmac-md5-96 | hmac-sha1-96);
  key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit authenticator value and 96-bit digest.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit authenticator value and a 96-bit digest.

The key can be one of the following:

- **ascii-text *key***—ASCII text key. With the **hmac-md5-96** option, the key contains 16 ASCII characters. With the **hmac-sha1-96** option, the key contains 20 ASCII characters.
- **hexadecimal *key***—Hexadecimal key. With the **hmac-md5-96** option, the key contains 32 hexadecimal characters. With the **hmac-sha1-96** option, the key contains 40 hexadecimal characters.

Configuring the Encryption Algorithm and Key

To configure IPsec encryption, include the **encryption** statement and specify an algorithm and key at the **[edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]** hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound |
  bi-directional)]
encryption {
  algorithm (des-cbc | 3des-cbc);
  key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 64 bits long.
- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.



NOTE: For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409. For **3des-cbc**, we recommend that the first 8 bytes not be the same as the second 8 bytes, and that the second 8 bytes be the same as the third 8 bytes.

The key can be one of the following:

- **ascii-text**—ASCII text key. With the **des-cbc** option, the key contains 8 ASCII characters. With the **3des-cbc** option, the key contains 24 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the **des-cbc** option, the key contains 16 hexadecimal characters. With the **3des-cbc** option, the key contains 48 hexadecimal characters.



NOTE: You cannot configure encryption when you use the AH protocol.

See Also • [Configuring Dynamic IPsec Security Associations on page 43](#)

Configuring Dynamic IPsec Security Associations

You configure dynamic SAs with a set of proposals that are negotiated by the security gateways. The keys are generated as part of the negotiation and do not need to be specified in the configuration. The dynamic SA includes one or more proposals, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer.

To configure a dynamic SA, include the **dynamic** statement at the **[edit security ipsec security-association *sa-name*]** hierarchy level. Specify an IPsec policy name, and optionally, a 32-packet or 64-packet replay window size.

```
[edit security ipsec security-association sa-name]
dynamic {
  ipsec-policy policy-name;
```

```
replay-window-size (32 | 64);  
}
```

See Also • [Configuring Manual IPsec Security Associations for an ES PIC on page 39](#)

Configuring an IKE Policy

- [Configuring an IKE Policy for Preshared Keys on page 44](#)
- [Example: Configuring an IKE Policy on page 46](#)

Configuring an IKE Policy for Preshared Keys

An IKE policy defines a combination of security parameters (IKE proposals) to be used during IKE negotiation. It defines a peer address, the preshared key for the given peer, and the proposals needed for that connection. During the IKE negotiation, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used. The configured preshared key must also match its peer.

You can create multiple, prioritized proposals at each peer to ensure that at least one proposal will match a remote peer's proposal.

First, you configure one or more IKE proposals; then you associate these proposals with an IKE policy. You can also prioritize a list of proposals used by IKE in the **policy** statement by listing the proposals you want to use, from first to last.

To configure an IKE policy, include the **policy** statement at the **[edit security ike]** hierarchy level and specify a peer address:

```
[edit security ike]  
policy ike-peer-address;
```



NOTE: The IKE policy peer address must be an IPsec tunnel destination address.

Tasks for configuring an IKE policy are:

1. [Configuring the Description for an IKE Policy on page 45](#)
2. [Configuring the Mode for an IKE Policy on page 45](#)
3. [Configuring the Preshared Key for an IKE Policy on page 45](#)
4. [Associating Proposals with an IKE Policy on page 45](#)

Configuring the Description for an IKE Policy

To specify a description for an IKE policy, include the **description** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address]  
description description;
```

Configuring the Mode for an IKE Policy

IKE policy has two modes: aggressive and main. By default, main mode is enabled. Main mode uses six messages, in three exchanges, to establish the IKE SA. (These three steps are IKE SA negotiation, a Diffie-Hellman key exchange, and authentication of the peer.) Main mode also allows a peer to hide its identity.

Aggressive mode also establishes an authenticated IKE SA and keys. However, aggressive mode uses half the number of messages, has less negotiation power, and does not provide identity protection. The peer can use the aggressive or main mode to start IKE negotiation; the remote peer accepts the mode sent by the peer.

To configure IKE policy mode, include the **mode** statement and specify **aggressive** or **main** at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address ]  
mode (aggressive | main);
```

For Junos OS in FIPS mode, the aggressive option for IKEv1 is not supported with the mode statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level.

Configuring the Preshared Key for an IKE Policy

IKE policy preshared keys authenticate peers. You must manually configure a preshared key, which must match that of its peer. The preshared key can be an ASCII text (alphanumeric) key or a hexadecimal key.

A local certificate is an alternative to the preshared key. A commit operation fails if either a preshared key or a local certificate is not configured.

To configure an IKE policy preshared key, include the **pre-shared-key** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address]  
pre-shared-key (ascii-text key | hexadecimal key);
```

Associating Proposals with an IKE Policy

The IKE policy proposal is a list of one or more proposals associated with an IKE policy.

To configure an IKE policy proposal, include the **proposals** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level and specify one or more proposal names:

```
[edit security ike policy ike-peer-address]  
proposals [ proposal-names ];
```

See Also • [Example: Configuring an IKE Policy on page 46](#)

Example: Configuring an IKE Policy

Define two IKE policies: policy 10.1.1.2 and policy 10.1.1.1. Each policy is associated with **proposal-1** and **proposal-2**.

```
[edit security]  
ike {  
  proposal proposal-1 {  
    authentication-method pre-shared-keys;  
    dh-group group1;  
    authentication-algorithm sha1;  
    encryption-algorithm 3des-cbc;  
    lifetime-seconds 1000;  
  }  
  proposal proposal-2 {  
    authentication-method pre-shared-keys;  
    dh-group group2;  
    authentication-algorithm md5;  
    encryption-algorithm des-cbc;  
    lifetime-seconds 10000;  
  }  
  proposal proposal-3 {  
    authentication-method rsa-signatures;  
    dh-group group2;  
    authentication-algorithm md5;  
    encryption-algorithm des-cbc;  
    lifetime-seconds 10000;  
  }  
  policy 10.1.1.2 {  
    mode main;  
    proposals [ proposal-1 proposal-2 ];  
    pre-shared-key ascii-text example-pre-shared-key;  
  }  
  policy 10.1.1.1 {  
    local-certificate certificate-filename;  
    local-key-pair private-public-key-file;  
    mode aggressive;  
    proposals [ proposal-2 proposal-3 ]  
    pre-shared-key hexadecimal 0102030abbcdd;  
  }  
}
```



NOTE: Updates to the current IKE proposal and policy configuration are not applied to the current IKE SA; updates are applied to new IKE SAs.

If you want the new updates to take immediate effect, you must clear the existing IKE security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IKE security association, see the [CLI Explorer](#).

See Also • [Configuring an IKE Policy for Preshared Keys on page 44](#)

Configuring an IPsec Proposal for an ES PIC

An IPsec proposal lists protocols and algorithms (security services) to be negotiated with the remote IPsec peer.

To configure an IPsec proposal and define its properties, include the following statements at the **[edit security ipsec]** hierarchy level:

```
[edit security ipsec]
proposal ipsec-proposal-name {
  authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
  description description ;
  encryption-algorithm (3des-cbc | des-cbc);
  lifetime-seconds seconds;
  protocol (ah | esp | bundle);
}
```

Tasks to configure an IPsec proposal for an ES PIC include:

- [Configuring the Authentication Algorithm for an IPsec Proposal on page 47](#)
- [Configuring the Description for an IPsec Proposal on page 48](#)
- [Configuring the Encryption Algorithm for an IPsec Proposal on page 48](#)
- [Configuring the Lifetime for an IPsec SA on page 48](#)
- [Configuring the Protocol for a Dynamic IPsec SA on page 49](#)

Configuring the Authentication Algorithm for an IPsec Proposal

To configure an IPsec authentication algorithm, include the **authentication-algorithm** statement at the **[edit security ipsec proposal ipsec-proposal-name]** hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name]
authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
```

The authentication algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit digest. Only 96 bits are used for authentication.

- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit digest. Only 96 bits are used for authentication.

Configuring the Description for an IPsec Proposal

To specify a description for an IPsec proposal, include the **description** statement at the **[edit security ipsec proposal *ipsec-proposal-name*]** hierarchy level:

```
[edit security ike policy ipsec-proposal-name]  
description description;
```

Configuring the Encryption Algorithm for an IPsec Proposal

To configure the IPsec encryption algorithm, include the **encryption-algorithm** statement at the **[edit security ipsec proposal *ipsec-proposal-name*]** hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name ]  
encryption-algorithm (3des-cbc | des-cbc);
```

The encryption algorithm can be one of the following:

- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 48 bits long.



NOTE: We recommend that you use the triple DES cipher block chaining (3DES-CBC) encryption algorithm.

Configuring the Lifetime for an IPsec SA

The IPsec lifetime option sets the lifetime of an IPsec SA. When the IPsec SA expires, it is replaced by a new SA (and SPI) or is terminated. A new SA has new authentication and encryption keys, and SPI; however, the algorithms may remain the same if the proposal is not changed. If you do not configure a lifetime and a lifetime is not sent by a responder, the lifetime is 28,800 seconds.

To configure the IPsec lifetime, include the **lifetime-seconds** statement and specify the number of seconds (180 through 86,400) at the **[edit security ipsec proposal *ipsec-proposal-name*]** hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name]  
lifetime-seconds seconds;
```



NOTE: When a dynamic SA is created, two types of lifetimes are used: hard and soft. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires. When you specify the lifetime, you specify a hard lifetime.

Configuring the Protocol for a Dynamic IPsec SA

The **protocol** statement sets the protocol for a dynamic SA. The ESP protocol can support authentication, encryption, or both. The AH protocol is used for strong authentication. AH also authenticates the IP packet. The **bundle** option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.

To configure the protocol for a dynamic SA, include the **protocol** statement at the **[edit security ipsec proposal *ipsec-proposal-name*]** hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name ] protocol (ah | esp | bundle);
```

See Also • [IPsec Configuration for an ES PIC Overview on page 35](#)

Configuring an IPsec Policy

- [Configuring the IPsec Policy for an ES PIC on page 49](#)
- [Example: Configuring an IPsec Policy on page 50](#)

Configuring the IPsec Policy for an ES PIC

An IPsec policy defines a combination of security parameters (IPsec proposals) used during IPsec negotiation. It defines Perfect Forward Secrecy (PFS) and the proposals needed for the connection. During the IPsec negotiation, IPsec looks for an IPsec proposal that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used.

You can create multiple, prioritized IPsec proposals at each peer to ensure that at least one proposal will match a remote peer's proposal.

First, you configure one or more IPsec proposals; then you associate these proposals with an IPsec policy. You can prioritize the proposals in the list by listing them in the order in which the IPsec policy uses them (first to last).

To configure an IPsec policy, include the **policy** statement at the **[edit security ipsec]** hierarchy level, specifying the policy name and one or more proposals you want to associate with this policy:

```
[edit security ipsec]
policy ipsec-policy-name {
  proposals [ proposal-names ];
}
```

Configuring Perfect Forward Secrecy

PFS provides additional security by means of a Diffie-Hellman key exchange shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys. This statement is optional.

To configure PFS, include the **perfect-forward-secrecy** statement and specify a Diffie-Hellman group at the **[edit security ipsec policy ipsec-policy-name]** hierarchy level:

```
[edit security ipsec policy ipsec-policy-name]
perfect-forward-secrecy {
  keys (group1 | group2);
}
```

The key can be one of the following:

- **group1**—Specify that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group2**—Specify that IKE use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

group2 provides more security than **group1**, but requires more processing time.

- See Also**
- [Example: Configuring an IPsec Policy on page 50](#)
 - [IPsec Configuration for an ES PIC Overview on page 35](#)

Example: Configuring an IPsec Policy

The following example shows how to configure an IPsec policy:

```
[edit security ipsec]
proposal dynamic-1 {
  protocol esp;
  authentication-algorithm hmac-md5-96;
  encryption-algorithm 3des-cbc;
  lifetime-seconds 6000;
}
proposal dynamic-2 {
  protocol esp;
  authentication-algorithm hmac-sha1-96;
  encryption-algorithm 3des-cbc;
```

```
lifetime-seconds 6000;
}
policy dynamic-policy-1 {
  perfect-forward-secrecy {
    keys group1;
  }
  proposals [ dynamic-1 dynamic-2 ];
}
security-association dynamic-sa1 {
  dynamic {
    replay-window-size 64;
    ipsec-policy dynamic-policy-1;
  }
}
```



NOTE: Updates to the current IPsec proposal and policy configuration are not applied to the current IPsec SA; updates are applied to new IPsec SAs.

If you want the new updates to take immediate effect, you must clear the existing IPsec security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IPsec security association, see the [CLI Explorer](#).

- See Also**
- [Configuring the IPsec Policy for an ES PIC on page 49](#)
 - [IPsec Configuration for an ES PIC Overview on page 35](#)

CHAPTER 4

Configuring IPsec Security Associations

- [Overview of IPsec on page 53](#)
- [IPsec Security Associations Overview on page 61](#)
- [Digital Certificates and Service Sets on page 62](#)
- [Configuring Security Associations on page 64](#)
- [Directing Traffic into an IPsec Tunnel on page 70](#)

Overview of IPsec

- [Security Associations Overview on page 53](#)
- [IKE Key Management Protocol Overview on page 54](#)
- [IPsec Requirements for Junos-FIPS on page 55](#)
- [Overview of IPsec on page 56](#)
- [IPsec-Enabled Line Cards on page 56](#)
- [Authentication Algorithms on page 57](#)
- [Encryption Algorithms on page 58](#)
- [IPsec Protocols on page 59](#)

Security Associations Overview

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

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

SA is negotiated first and then used to protect the negotiations that determine the dynamic IPsec SAs.

- Set up user-level tunnels or SAs, including tunnel attribute negotiations and key management. These tunnels can also be refreshed and terminated on top of the same secure channel.

The Junos OS implementation of IPsec supports two modes of security (transport mode and tunnel mode).

- See Also**
- *IKE Key Management Protocol Overview*
 - *IPsec Requirements for Junos-FIPS*
 - *[edit security] Hierarchy Level*

IKE Key Management Protocol Overview

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

IKE does the following:

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

IKE occurs over two phases. In the first phase, it negotiates security attributes and establishes shared secrets to form the bidirectional IKE SA. In the second phase, inbound and outbound IPsec SAs are established. The IKE SA secures the exchanges in the second phase. IKE also generates keying material, provides Perfect Forward Secrecy, and exchanges identities.



NOTE: Starting in Junos OS Release 14.2, when you perform an SNMP walk of the `jnxIkeTunnelEntry` object in the `jnxIkeTunnelTable` table, the `Request failed: OID not increasing` error message might be generated. This problem occurs only when simultaneous Internet Key Exchange security associations (IKE SAs) are created, which occurs when both ends of the SA initiate IKE SA negotiations at the same time. When an SNMP MIB walk is performed to display IKE SAs, the `snmpwalk` tool expects the object identifiers (OIDs) to be in increasing order. However, in the case of simultaneous IKE SAs, the OIDs in the SNMP table might not be in increasing order. This behavior occurs because the tunnel IDs, which are part of the OIDs, are allocated based on the initiator of the IKE SA, which can be on either side of the IKE tunnel.

The following is an example of an SNMP MIB walk that is performed on IKE simultaneous SAs:

```
jnxIkeTunnelLocalRole."ipsec_ss_cust554".ipv4."192.0.2.41".47885 = INTEGER:
responder(2)    >>> This is Initiator SA
jnxIkeTunnelLocalRole."ipsec_ss_cust554".ipv4."192.0.2.41".47392 = INTEGER:
initiator(1)    >>> This is Responder's SA
```

The OID comparison fails when the SNMP walk is tunnel ID (47885 and 47392). It cannot be ensured when an SNMP walk is performed that the tunnel IDs are in increasing order because tunnels might be initiated from either side.

To work around this problem, the SNMP MIB walk contains an option, `-Cc`, to disable check for increasing OIDs. The following is an example of the MIB walk performed on the `jnxIkeTunnelEntry` table with the `-Cc` option:

```
snmpwalk -Os -Cc -c public -v 1 vira jnxIkeTunnelEntry
```

- See Also**
- *Security Associations Overview*
 - *IPsec Requirements for Junos-FIPS*
 - *[edit security] Hierarchy Level*

IPsec Requirements for Junos-FIPS

In a Junos-FIPS environment, hardware configurations with two Routing Engines must be configured to use IPsec and a private routing instance for all communications between the Routing Engines. IPsec communication between the Routing Engines and AS II FIPS PICs is also required.

- See Also**
- *Security Associations Overview*
 - *IKE Key Management Protocol Overview*

- [\[edit security\] Hierarchy Level](#)

Overview of IPsec

IP Security (IPsec) is a standards based framework for ensuring secure private communication over IP networks. IPsec provides a secure way to authenticate senders and encrypt IP version 4 (IPv4) and version 6 (IPv6) traffic between network devices, such as routers and hosts. IPsec includes data integrity, sender authentication, source data confidentiality, and protection against data replay.

The main concepts you need to understand are as follows:

- [IPsec-Enabled Line Cards on page 56](#)
- [Authentication Algorithms on page 57](#)
- [Encryption Algorithms on page 58](#)
- [IPsec Protocols on page 59](#)
- [IPsec Security Associations on page 61](#)
- [IPsec Modes on page 61](#)
- [Digital Certificates on page 62](#)
- [Service Sets on page 64](#)

IPsec-Enabled Line Cards

The first choice you need to make when implementing IPsec on a Junos OS-based router is the type of line card you wish to use. The term line card includes Physical Interface Cards (PICs), Modular Interface Cards (MICs), Dense Port Concentrators (DPCs), and Modular Port Concentrators (MPCs). The following line cards support IPsec implementation.



NOTE: See the specific hardware documentation for your router to determine if the line cards on that router support IPsec.

The following line cards support IPsec:

- The Encryption Services (ES) PIC provides encryption services and software support for IPsec.
- The Adaptive Services (AS) PIC and the Adaptive Services (AS) II PIC provide IPsec services and other services, such as Network Address Translation (NAT) and stateful firewall.
- The AS II Federal Information Processing Standards (FIPS) PIC is a special version of the AS PIC that communicates securely with the Routing Engine by using internal IPsec. You must configure IPsec on the AS II FIPS PIC when you enable FIPS mode on the router. For more information about implementing IPsec on an AS II FIPS PIC installed

in a router configured in FIPS mode, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

- The Multiservices PICs supply hardware acceleration for an array of packet processing-intensive services. These services include IPsec services and other services, such as stateful firewall, NAT, IPsec, anomaly detection, and tunnel services.
- The Multiservices Dense Port Concentrators (DPCs) provide IPsec services.
- The Multiservices Modular Port Concentrators (MS-MPCs) support IPsec services.
- The Multiservices Modular Interface Cards (MS-MICs) support IPsec services.



NOTE: Junos OS extension-provider packages, including the IPsec service package, come preinstalled and preconfigured on MS-MPCs and MS-MICs.

- See Also**
- [Overview of IPSec on page 56](#)
 - [Considering General IPsec Issues on page 31](#)
 - *Understanding Services PICs*
 - *Enabling Service Packages*
 - *Multiservices MIC and Multiservices MPC (MS-MIC and MS-MPC) Overview*

Authentication Algorithms

Authentication is the process of verifying the identity of the sender. Authentication algorithms use a shared key to verify the authenticity of the IPsec devices. The Junos OS uses the following authentication algorithms:

- Message Digest 5 (MD5) uses a one-way hash function to convert a message of arbitrary length to a fixed-length message digest of 128 bits. Because of the conversion process, it is mathematically infeasible to calculate the original message by computing it backwards from the resulting message digest. Likewise, a change to a single character in the message will cause it to generate a very different message digest number.

To verify that the message has not been tampered with, the Junos OS compares the calculated message digest against a message digest that is decrypted with a shared key. The Junos OS uses the MD5 hashed message authentication code (HMAC) variant that provides an additional level of hashing. MD5 can be used with authentication header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE).

- Secure Hash Algorithm 1 (SHA-1) uses a stronger algorithm than MD5. SHA-1 takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest ensures that the data has not been changed and that it originates from the correct source. The Junos OS uses the SHA-1 HMAC variant that provides an additional level of hashing. SHA-1 can be used with AH, ESP, and IKE.
- SHA-256, SHA-384, and SHA-512 (sometimes grouped under the name SHA-2) are variants of SHA-1 and use longer message digests. The Junos OS supports the SHA-256

version of SHA-2, which can process all versions of Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES) encryption.

- See Also**
- *Understanding Junos VPN Site Secure*
 - [Encryption Algorithms on page 58](#)

Encryption Algorithms

Encryption encodes data into a secure format so that it cannot be deciphered by unauthorized users. Like authentication algorithms, a shared key is used with encryption algorithms to verify the authenticity of the IPsec devices. The Junos OS uses the following encryption algorithms:

- Data Encryption Standard cipher-block chaining (DES-CBC) is a symmetric secret-key block algorithm. DES uses a key size of 64 bits, where 8 bits are used for error detection and the remaining 56 bits provide encryption. DES performs a series of simple logical operations on the shared key, including permutations and substitutions. CBC takes the first block of 64 bits of output from DES, combines this block with the second block, feeds this back into the DES algorithm, and repeats this process for all subsequent blocks.
- Triple DES-CBC (3DES-CBC) is an encryption algorithm that is similar to DES-CBC, but provides a much stronger encryption result because it uses three keys for 168-bit (3 x 56-bit) encryption. 3DES works by using the first key to encrypt the blocks, the second key to decrypt the blocks, and the third key to re-encrypt the blocks.
- Advanced Encryption Standard (AES) is a next-generation encryption method based on the Rijndael algorithm developed by Belgian cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. It uses a 128-bit block and three different key sizes (128, 192, and 256 bits). Depending on the key size, the algorithm performs a series of computations (10, 12, or 14 rounds) that include byte substitution, column mixing, row shifting, and key addition. The use of AES in conjunction with IPsec is defined in RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*.
- Starting In Junos OS Release 17.3R1, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) is supported for MS-MPCs and MS-MICs. However, in Junos FIPS mode, AES-GCM is not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, AES-GCM is supported in Junos FIPS mode. AES-GCM is an authenticated encryption algorithm designed to provide both authentication and privacy. AES-GCM uses universal hashing over a binary Galois field to provide authenticated encryption and allows authenticated encryption at data rates of tens of Gbps.

- See Also**
- *Understanding Junos VPN Site Secure*
 - *Configuring IKE Proposals*
 - *Configuring IPsec Proposals*

IPsec Protocols

IPsec protocols determine the type of authentication and encryption applied to packets that are secured by the router. The Junos OS supports the following IPsec protocols:

- **AH**—Defined in RFC 2402, AH provides connectionless integrity and data origin authentication for IPv4 and IPv6 packets. It also provides protection against replays. AH authenticates as much of the IP header as possible, as well as the upper-level protocol data. However, some IP header fields might change in transit. Because the value of these fields might not be predictable by the sender, they cannot be protected by AH. In an IP header, AH can be identified with a value of **51** in the **Protocol** field of an IPv4 packet and the **Next Header** field of an IPv6 packet. An example of the IPsec protection offered by AH is shown in [Figure 2 on page 59](#).



NOTE: AH is not supported on the T Series, M120, and M320 routers.

Figure 2: AH Protocol

Header format

Byte 0	Byte 1	Byte 2	Byte 3
Next header	Payload length	Reserved	
Security Parameters Index (SPI)			
Sequence number			
Authentication data (variable)			

Original IPv4 packet before AH is applied

Original IP header	TCP header	Data
--------------------	------------	------

IPv4 packet after AH transport mode is applied

Original IP header	AH header	TCP header	Data
Authenticating			

IPv4 packet after AH tunnel mode is applied

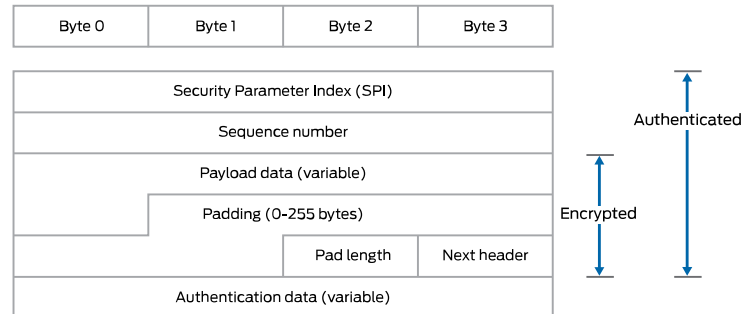
New IP header	AH header	Original IP header	TCP header	Data
Authenticating				

g015522

- **ESP**—Defined in RFC 2406, ESP can provide encryption and limited traffic flow confidentiality, or connectionless integrity, data origin authentication, and an anti-replay service. In an IP header, ESP can be identified a value of **50** in the **Protocol** field of an IPv4 packet and the **Next Header** field of an IPv6 packet. An example of the IPsec protection offered by ESP is shown in [Figure 3 on page 60](#).

Figure 3: ESP Protocol

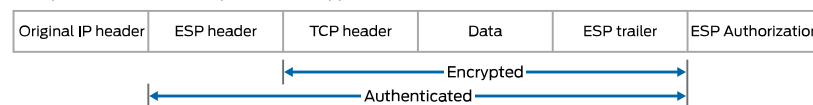
Header format



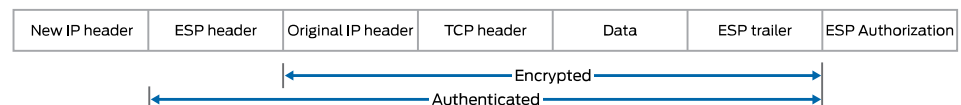
Original IPv4 packet before ESP is applied



IPv4 packet after ESP transport mode is applied



IPv4 packet after ESP tunnel mode is applied



8015521

- **Bundle**—When you compare AH with ESP, there are some benefits and shortcomings in both protocols. ESP provides a decent level of authentication and encryption, but does so only for part of the IP packet. Conversely, although AH does not provide encryption, it does provide authentication for the entire IP packet. Because of this, the Junos OS offers a third form of IPsec protocol called a protocol bundle. The bundle option offers a hybrid combination of AH authentication with ESP encryption.

- See Also**
- *Understanding Junos VPN Site Secure*
 - *Configuring IPsec Proposals*
 - *Configuring Security Associations*
 - *protocol (IPsec)*

IPsec Security Associations Overview

- [IPsec Security Associations on page 61](#)
- [IPsec Modes on page 61](#)

IPsec Security Associations

Another IPsec consideration is the type of security association (SA) that you wish to implement. An SA is a set of IPsec specifications that are negotiated between devices that are establishing an IPsec relationship. These specifications include preferences for the type of authentication, encryption, and IPsec protocol that should be used when establishing the IPsec connection. An SA can be either unidirectional or bidirectional, depending on the choices made by the network administrator. An SA is uniquely identified by a Security Parameter Index (SPI), an IPv4 or IPv6 destination address, and a security protocol (AH or ESP) identifier.

You can configure IPsec with a preset, preshared manual SA or use IKE to establish a dynamic SA. Manual SAs require you to specify all the IPsec requirements up front. Conversely, IKE dynamic SAs typically contain configuration defaults for the highest levels of authentication and encryption.

IPsec Modes

When configuring IPsec, the last major consideration is the type of IPsec mode you wish to implement in your network. The Junos OS supports the following IPsec modes:

- Tunnel mode is supported for both AH and ESP in the Junos OS and is the usual choice for a router. In tunnel mode, the SA and associated protocols are applied to tunneled IPv4 or IPv6 packets. For a tunnel mode SA, an outer IP header specifies the IPsec processing destination, and an inner IP header specifies the ultimate destination for the packet. The security protocol header appears after the outer IP header, and before the inner IP header. In addition, there are slight differences for tunnel mode when you implement it with AH and ESP:
 - For AH, portions of the outer IP header are protected, as well as the entire tunneled IP packet.
 - For ESP, only the tunneled packet is protected, not the outer header.

When one side of a security association is a security gateway (such as a router), the SA must use tunnel mode. However, when traffic (for example, SNMP commands or BGP sessions) is destined for a router, the system acts as a host. Transport mode is allowed in this case because the system does not act as a security gateway and does not send or receive transit traffic.

- Transport mode provides a security association between two hosts. In transport mode, the protocols provide protection primarily for upper layer protocols. For IPv4 and IPv6 packets, a transport mode security protocol header appears immediately after the IP header and any options, and before any higher layer protocols (for example, TCP or UDP). There are slight differences for transport mode when you implement it with AH and ESP:

- For AH, selected portions of the IP header are protected, as well as selected portions of the extension headers and selected options within the IPv4 header.
- For ESP, only the higher layer protocols are protected, not the IP header or any extension headers preceding the ESP header.



NOTE: Support for IPSec transport mode is primarily limited to routing authentication and to certain configurations only application when Junos FIPs code is used.

- See Also**
- [Overview of IPSec on page 56](#)
 - [Configuring Security Associations on page 64](#)
 - [Understanding OSPFv3 Authentication](#)
 - [Example: Configuring IPsec Authentication for an OSPF Interface](#)

Digital Certificates and Service Sets

- [Digital Certificates on page 62](#)
- [Service Sets on page 64](#)

Digital Certificates

For small networks, the use of preshared keys in an IPSec configuration is often sufficient. However, as a network grows, it can become a challenge to add new preshared keys on the local router and all new and existing IPSec peers. One solution for scaling an IPSec network is to use digital certificates.

A digital certificate implementation uses the public key infrastructure (PKI), which requires you to generate a key pair consisting of a public key and a private key. The keys are created with a random number generator and are used to encrypt and decrypt data. In networks that do not use digital certificates, an IPSec-enabled device encrypts data with the private key and IPSec peers decrypt the data with the public key.

With digital certificates, the key sharing process requires an additional level of complexity. First, you and your IPSec peers request a certificate authority (CA) to send you a CA certificate that contains the public key of the CA. Next, you request the CA to enroll a local digital certificate that contains your public key and some additional information. When the CA processes your request, it signs your local certificate with the private key of the CA. Then you install the CA certificate and the local certificate in your local router and load the CA certificate in the remote devices before you can establish IPSec tunnels with your peers.

When you request a peering relationship with an IPSec peer, the peer receives a copy of your local certificate. Because the peer already has the CA certificate loaded, it can use the CA's public key contained in the CA certificate to decrypt your local certificate that has been signed by the CA's private key. As a result, the peer now has a copy of your

public key. The peer encrypts data with your public key before sending it to you. When your local router receives the data, it decrypts the data with your private key.

In the Junos OS, you must implement the following steps to be able to initially use digital certificates:

- Configure a CA profile to request CA and local digital certificates—The profile contains the name and URL of the CA or registration authority (RA), as well as some retry timer settings.
- Configure certificate revocation list support—A certificate revocation list (CRL) contains a list of certificates canceled before their expiration date. When a participating peer uses a CRL, the CA acquires the most recently issued CRL and checks the signature and validity of a peer's digital certificate. You can request and load CRLs manually, configure an LDAP server to handle CRL processing automatically, or disable CRL processing that is enabled by default.
- Request a digital certificate from the CA—The request can be made either online or manually. Online CA digital certificate requests use the Simple Certificate Enrollment Protocol (SCEP) format. If you request the CA certificate manually, you must also load the certificate manually.
- Generate a private/public key pair—The public key is included in the local digital certificate and the private key is used to decrypt data received from peers.
- Generate and enroll a local digital certificate—The local certificate can be processed online using SCEP or generated manually in the Public-Key Cryptography Standards #10 (PKCS-10) format. If you create the local certificate request manually, you must also load the certificate manually.
- Apply the digital certificate to an IPsec configuration—To activate a local digital certificate, you configure the IKE proposal to use digital certificates instead of preshared keys, reference the local certificate in the IKE policy, and identify the CA in the service set.

Optionally, you can do the following:

- Configure the digital certificate to automatically reenroll—Starting in Junos OS Release 8.5, you can configure automatic reenrollment for digital certificates.
- Monitor digital certificate events and delete certificates and requests—You can issue operational mode commands to monitor IPsec tunnels established using digital certificates and delete certificates or requests.

For more details on managing digital certificates, configuring them in an IPsec service set, and monitoring and clearing them, see [“Using Digital Certificates for IPsec” on page 73](#) and [“Example: AS PIC IKE Dynamic SA with Digital Certificates Configuration” on page 145](#).

Service Sets

The Adaptive Services PIC supports two types of service sets when you configure IPsec tunnels. Because they are used for different purposes, it is important to know the differences between these service set types.

- Next-hop service set—Supports multicast and multicast-style dynamic routing protocols (such as OSPF) over IPsec. Next-hop service sets allow you to use *inside* and *outside* logical interfaces on the Adaptive Services PIC to connect with multiple routing instances. They also allow the use of Network Address Translation (NAT) and stateful firewall capabilities. However, next-hop service sets do not monitor Routing Engine traffic by default and require configuration of multiple service sets to support traffic from multiple interfaces.
- Interface service set—Applied to a physical interface and similar to a stateless firewall filter. They are easy to configure, can support traffic from multiple interfaces, and can monitor Routing Engine traffic by default. However, they cannot support dynamic routing protocols or multicast traffic over the IPsec tunnel.

In general, we recommend that you use next-hop service sets because they support routing protocols and multicast over the IPsec tunnel, they are easier to understand, and the routing table makes forwarding decisions without administrative intervention.

- See Also**
- [Understanding Junos VPN Site Secure](#)
 - [Configuring Junos VPN Site Secure or IPsec VPN](#)

Configuring Security Associations

- [Configuring Security Associations on page 64](#)
- [Configuring Manual SAs on page 64](#)
- [Configuring IKE Dynamic SAs on page 66](#)

Configuring Security Associations

The first IPsec configuration step is to select a type of security association (SA) for your IPsec connection. You must statically configure all specifications for manual SAs, but you can rely on some defaults when you configure an IKE dynamic SA. To configure a security association, see the following sections.

Configuring Manual SAs

On the ES PIC, you configure a manual security association at the **[edit security ipsec security-association *name*]** hierarchy level. Include your choices for authentication, encryption, direction, mode, protocol, and SPI. Be sure that these choices are configured exactly the same way on the remote IPsec gateway.

```
[edit security]
ipsec {
```

```

security-association sa-name {
  description description;
  manual {
    direction (inbound | outbound | bidirectional) {
      authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      auxiliary-spi auxiliary-spi;
      encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
      }
      protocol (ah | esp | bundle);
      spi spi-value;
    }
  }
  mode (tunnel | transport);
}

```

On the AS and MultiServices PICs, you configure a manual security association at the **[edit services ipsec-vpn rule *rule-name*]** hierarchy level. Include your choices for authentication, encryption, direction, protocol, and SPI. Be sure that these choices are configured exactly the same way on the remote IPsec gateway.

```

[edit services ipsec-vpn]
rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      destination-address address;
      source-address address;
    }
    then {
      backup-remote-gateway address;
      clear-dont-fragment-bit;
      manual {
        direction (inbound | outbound | bidirectional) {
          authentication {
            algorithm (hmac-md5-96 | hmac-sha1-96);
            key (ascii-text key | hexadecimal key);
          }
          auxiliary-spi spi-value;
          encryption {
            algorithm algorithm; # This can be aes-128-cbc, aes-192-cbc,
            # aes-256-cbc, des-cbc, or 3des-cbc.
            key (ascii-text key | hexadecimal key);
          }
          protocol (ah | bundle | esp);
          spi spi-value;
        }
      }
    }
  }
  no-anti-replay;
}

```

```

        remote-gateway address;
        syslog;
    }
}
rule-set rule-set-name {
    [ rule rule-names ];
}

```

Configuring IKE Dynamic SAs

On the ES PIC, you configure an IKE dynamic SA at the **[edit security ike]** and **[edit security ipsec]** hierarchy levels. Include your choices for IKE policies and proposals, which include options for authentication algorithms, authentication methods, Diffie-Hellman groups, encryption, IKE modes, and preshared keys. The IKE policy must use the IP address of the remote end of the IPsec tunnel as the policy name. Also, include your choices for IPsec policies and proposals, which include options for authentication, encryption, protocols, Perfect Forward Secrecy (PFS), and IPsec modes. Be sure that these choices are configured exactly the same way on the remote IPsec gateway.

```

[edit security]
ike {
    proposal ike-proposal-name {
        authentication-algorithm (md5 | sha1 | sha-256 | sha-384);
        authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
        description description;
        dh-group (group1 | group2);
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        lifetime-seconds seconds;
    }
    policy ike-peer-address {
        description description;
        encoding (binary | pem);
        identity identity-name;
        local-certificate certificate-filename;
        local-key-pair private-public-key-file;
        mode (aggressive | main);
        pre-shared-key (ascii-text key | hexadecimal key);
        proposals [ proposal-names ];
    }
}
ipsec {
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96 | hmac-sha-256-128);
        description description;
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol (ah | esp | bundle);
    }
    policy ipsec-policy-name {
        description description;
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
    }
}

```

```

    }
    proposals [ proposal-names ];
  }
  security-association sa-name {
    description description;
    dynamic {
      ipsec-policy policy-name;
      replay-window-size (32 | 64);
    }
    mode (tunnel | transport);
  }
}

```

On the AS and MultiServices PICs, you configure an IKE dynamic security association at the `[edit services ipsec-vpn ike]`, `[edit services ipsec-vpn ipsec]`, and `[edit services ipsec-vpn rule rule-name]` hierarchy levels. Include your choices for IKE policies and proposals, which include options for authentication algorithms, authentication methods, Diffie-Hellman groups, encryption, IKE modes, and preshared keys. Also, include your choices for IPsec policies and proposals, which include options for authentication, encryption, protocols, PFS, and IPsec modes. Be sure that these choices are configured exactly the same way on the remote IPsec gateway.

If you choose not to explicitly configure IKE and IPsec policies and proposals on the AS and MultiServices PICs, your configuration can default to some preset values. These default values are shown in [Table 7 on page 67](#).

Table 7: IKE and IPsec Proposal and Policy Default Values for the AS and MultiServices PICs

IKE Policy Statement	Default Value
<code>mode</code>	<code>main</code>
<code>proposals</code>	<code>default</code>
IKE Proposal Statement	Default Value
<code>authentication-algorithm</code>	<code>sha1</code>
<code>authentication-method</code>	<code>pre-shared-keys</code>
<code>dh-group</code>	<code>group2</code>
<code>encryption-algorithm</code>	<code>3des-cbc</code>
<code>lifetime-seconds</code>	<code>3600 (seconds)</code>
IPsec Policy Statement	Default Value
<code>perfect-forward-secrecy keys</code>	<code>group2</code>
<code>proposals</code>	<code>default</code>

Table 7: IKE and IPsec Proposal and Policy Default Values for the AS and MultiServices PICs (continued)

IKE Policy Statement	Default Value
IPsec Proposal Statement	Default Value
authentication-algorithm	hmac-sha1-96
encryption-algorithm	3des-cbc
lifetime-seconds	28800 (seconds)
protocol	esp



NOTE: If you use the default IKE and IPsec policy and proposal values preset within the AS and MultiServices PICs, you must explicitly configure an IKE policy and include a preshared key. This is because the **pre-shared-keys** authentication method is one of the preset values in the default IKE proposal.



NOTE: Starting in Junos OS release 14.2, in an environment in which Juniper Networks MX Series routers interoperate with Cisco ASA devices, IKE security associations (SAs) and IPsec SAs are deleted immediately on the Cisco ASA devices, but they are retained on the MX Series routers. As a result, 100 percent traffic loss occurs on the MX routers when traffic is initiated from either the MX Series routers or Cisco ASA devices. This problem of excessive traffic loss occurs when a service PIC is restarted on MX Series routers, a line card is restarted on MX series routers, or when a shutdown/no shutdown command sequence or a change in speed setting is performed on the Cisco ASA devices. To prevent this problem of the preservation of IKE and IPsec SAs in such a deployment, you must manually delete the IPsec and IKE SAs by entering the **clear ipsec security-associations** and **clear ike security-associations** commands respectively.

If you decide to configure values manually, the following information shows the complete statement hierarchy and options for dynamic IKE SAs on the AS and MultiServices PICs:

```
[edit services ipsec-vpn]
ike {
  proposal proposal-name {
    authentication-algorithm (md5 | sha1 | sha256);
    authentication-method (pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group2);
    encryption-algorithm algorithm; # This can be aes-128-cbc, aes-192-cbc,
    # aes-256-cbc, des-cbc, or 3des-cbc.
    lifetime-seconds seconds;
```



```

}
policy policy-name {
  description description;
  local-id {
    ipv4_addr [ values ];
    key_id [ values ];
  }
  local-certificate certificate-id-name;
  mode (aggressive | main);
  pre-shared-key (ascii-text key | hexadecimal key);
  proposals [ proposal-names ];
  remote-id {
    ipv4_addr [ values ];
    key_id [ values ];
  }
}
}
ipsec {
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    description description;
    encryption-algorithm algorithm; # This can be aes-128-cbc, aes-192-cbc,
    # aes-256-cbc, des-cbc, or 3des-cbc.
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
  }
  policy policy-name {
    description description;
    perfect-forward-secrecy {
      keys (group1 | group2);
    }
    proposals [ proposal-names ];
  }
}
rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      destination-address address;
      source-address address;
    }
    then {
      backup-remote-gateway address;
      clear-dont-fragment-bit;
      dynamic {
        ike-policy policy-name;
        ipsec-policy policy-name;
      }
      no-anti-replay;
      remote-gateway address;
      syslog;
    }
  }
}
rule-set rule-set-name {

```

```
[ rule rule-names ];
}
```

Release History Table

Release	Description
14.2	Starting in Junos OS release 14.2, in an environment in which Juniper Networks MX Series routers interoperate with Cisco ASA devices, IKE security associations (SAs) and IPsec SAs are deleted immediately on the Cisco ASA devices, but they are retained on the MX Series routers.

Directing Traffic into an IPsec Tunnel

- [Using a Filter to Select Traffic to Be Secured on page 70](#)
- [Applying the Filter or Service Set to the Interface Receiving Traffic to Be Secured on page 72](#)

Using a Filter to Select Traffic to Be Secured

For the ES PIC, you need to configure a firewall filter to direct traffic into the IPsec tunnel. To apply a security association to traffic that matches a firewall filter, include the **ipsec-sa sa-name** statement at the **[edit firewall filter *filter-name* term *term-name* then]** hierarchy level.

```
[edit firewall filter filter-name]
term term-name {
  from {
    source-address {
      ip-address;
    }
    destination-address {
      ip-address;
    }
  }
  then {
    count counter-name;
    ipsec-sa sa-name;
  }
}
term other {
  then accept;
}
```

For the AS and MultiServices PICs, you do not need to configure a separate firewall filter. A filter is already built into the IPsec VPN **rule** statement at the **[edit services ipsec-vpn]** hierarchy level. To apply a security association to traffic that matches the IPsec VPN rule, include the **dynamic** or **manual** statement at the **[edit services rule *rule-name* term *term-name* then]** hierarchy level. To specify whether the rule should match input or output traffic, include the **match-direction** statement at the **[edit services rule *rule-name*]** hierarchy level.

After defining the rules for your IPsec VPNs, you must apply the rules to a service set. To do this, include the `ipsec-vpn-rules rule-name` statement at the `[edit services service-set service-set-name]` hierarchy level. Include an IPv4 or IPv6 IPsec gateway with the `local-gateway local-ip-address` statement at the `[edit services service-set service-set-name]` hierarchy level.

Also, you must select either a single interface or a pair of interfaces that participate in IPsec. To select a single interface, include the interface-service `interface-name` statement at the `[edit services service-set service-set-name]` hierarchy level. To select a pair of interfaces and a next hop, include the `next-hop-service` statement at the `[edit services service-set service-set-name]` hierarchy level and specify an inside interface and an outside interface. Only next-hop service sets support IPsec within Layer 3 VPNs and use of routing protocols over the IPsec tunnel.

```
[edit services]
service-set service-set-name {
  interface-service {
    service-interface interface-name;
  }
  next-hop-service {
    inside-service-interface interface-name;
    outside-service-interface interface-name;
  }
  ipsec-vpn-options {
    local-gateway local-ip-address <routing-instance instance-name>;
    trusted-ca ca-profile-name;
  }
  ipsec-vpn-rules rule-name;
}
ipsec-vpn {
  rule rule-name {
    term term-name {
      from {
        source-address {
          ip-address;
        }
        destination-address {
          ip-address;
        }
      }
      then {
        remote-gateway remote-ip-address;
        (dynamic | manual);
      }
    }
    match-direction output;
  }
}
```

Applying the Filter or Service Set to the Interface Receiving Traffic to Be Secured

For the ES PIC, apply your firewall filter on the input interface receiving the traffic that you wish to send to the IPsec tunnel. To do this, include the **filter** statement at the **[edit interfaces *interface-name* unit *unit-number* family inet]** hierarchy level.

```
[edit interfaces interface-name unit unit-number family inet]
filter {
  input filter-name;
}
```

For the AS and MultiServices PICs, apply your IPsec-based interface service set to the input interface receiving the traffic that you wish to send to the IPsec tunnel. To do this, include the **service-set *service-set-name*** statement at the **[edit interfaces *interface-name* unit *unit-number* family inet service (input | output)]** hierarchy level.

```
[edit interfaces interface-name unit unit-number family inet]
service {
  input {
    service-set service-set-name;
  }
  output {
    service-set service-set-name;
  }
}
```

To configure a next-hop-based service set on the AS and MultiServices PICs, include the **service-domain** statement at the **[edit interfaces *interface-name* unit *unit-number*]** hierarchy level and specify one logical interface on the AS PIC as an inside interface and a second logical interface on the AS PIC as an outside interface.

```
[edit interfaces sp-fpc/pic/port]
unit 0 {
  family inet {
    address ip-address;
  }
}
unit 1 {
  family inet;
  service-domain inside;
}
unit 2 {
  family inet;
  service-domain outside;
}
```

CHAPTER 5

Using Digital Certificates for IPsec

- [Using Digital Certificates for IPsec on page 73](#)
- [Requesting a CA Digital Certificate on page 75](#)
- [Monitoring and Clearing Digital Certificates on page 77](#)

Using Digital Certificates for IPsec

- [Using Digital Certificates for IPsec on page 73](#)
- [Configuring a CA Profile on page 74](#)
- [Configuring a Certificate Revocation List on page 74](#)

Using Digital Certificates for IPsec

A popular way for network administrators to scale an IPsec network is to use digital certificates instead of preshared keys. To enable digital certificates in your network, you need to use a combination of operational mode commands and configuration statements. The following tasks enable you to implement digital certificates on AS and MultiServices PICs installed in M Series and T Series routers:

- [Configuring a CA Profile on page 74](#)
- [Configuring a Certificate Revocation List on page 74](#)
- [Requesting a CA Digital Certificate on page 75](#)
- [Generating a Private/Public Key Pair on page 76](#)
- [Generating and Enrolling a Local Digital Certificate on page 76](#)
- [Applying the Local Digital Certificate to an IPsec Configuration on page 76](#)
- [Configuring Automatic Reenrollment of Digital Certificates on page 77](#)
- [Monitoring Digital Certificates on page 77](#)
- [Clearing Digital Certificates on page 78](#)

See Also • [Digital Certificates on page 62](#)

Configuring a CA Profile

The CA profile contains the name and URL of the CA or RA, as well as some retry timer settings. CA certificates issued by Entrust, VeriSign, and Microsoft are all compatible with M Series, and T Series routers. To configure the domain name of the CA or RA, include the **ca-identity** statement at the **[edit security pki ca-profile *ca-profile-name*]** hierarchy level. To configure the URL of the CA, include the **url** statement at the **[edit security pki ca-profile *ca-profile-name* enrollment]** hierarchy level. To configure the number of enrollment attempts the router should perform, include the **retry** statement at the **[edit security pki ca-profile *ca-profile-name* enrollment]** hierarchy level. To configure the amount of time the router should wait between enrollment attempts, include the **retry-interval** statement at the **[edit security pki ca-profile *ca-profile-name* enrollment]** hierarchy level.

```
[edit security pki]
ca-profile ca-profile-name {
  ca-identity ca-identity;
  enrollment {
    url url-name;
    retry number-of-enrollment-attempts; # The range is 0 though 100 attempts.
    retry-interval seconds; # The range is 0 though 3600 seconds.
  }
}
```



NOTE: When you delete the entire public key infrastructure (PKI) configuration, all the CA certificates in the device are not deleted as expected. These CA certificates are accessible after you create the CA profiles again.

Configuring a Certificate Revocation List

A certificate revocation list (CRL) contains a list of digital certificates that have been canceled before their expiration date. When a participating peer uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL. By default, CRL verification is enabled on any CA profile running on Junos OS Release 8.1 or later. To disable CRL verification, include the **disable** statement at the **[edit security pki ca-profile *ca-profile-name* revocation-check]** hierarchy level.

To specify the URL for the Lightweight Directory Access Protocol (LDAP) server where your CA stores its current CRL, include the **url** statement at the **[edit security pki ca-profile *ca-profile-name* revocation-check *crl*]** hierarchy level. If the LDAP server requires a password to access the CRL, include the **password** statement at the **[edit security pki ca-profile *ca-profile-name* revocation-check *crl* *url*]** hierarchy level.



NOTE: You do not need to specify a URL for the LDAP server if the certificate includes a certificate distribution point (CDP). The CDP is a field within the certificate that contains information about how to retrieve the CRL for the certificate. The router uses this information to download the CRL automatically. Any LDAP URL you configure takes precedence over the CDP included in the certificate.

If you manually downloaded the CRL, you must manually install it on the router. To manually install the CRL, issue the `request security pki crl load ca-profile ca-profile-name filename path/filename` command.

To configure the time interval between CRL updates, include the `refresh-interval` statement at the `[edit security ca-profile ca-profile-name revocation-check crl]` hierarchy level.

To override the default behavior and permit IPsec peer authentication to continue when the CRL fails to download, include the `disable on-download-failure` statement at the `[edit security ca-profile ca-profile-name revocation-check crl]` hierarchy level.

```
[edit security pki ca-profile ca-profile-name]
revocation-check {
  disable;
  crl {
    disable on-download-failure;
    refresh-interval number-of-hours { # The range is 0 through 8784 hours.
      url {
        url-name;
        password;
      }
    }
  }
}
```

Requesting a CA Digital Certificate

- [Requesting a CA Digital Certificate on page 75](#)
- [Generating a Private/Public Key Pair on page 76](#)
- [Generating and Enrolling a Local Digital Certificate on page 76](#)
- [Applying the Local Digital Certificate to an IPsec Configuration on page 76](#)
- [Configuring Automatic Reenrollment of Digital Certificates on page 77](#)

Requesting a CA Digital Certificate

You can request a CA digital certificate either online or manually. To request a digital certificate from a CA or RA online by using SCEP, issue the `request security pki ca-certificate enroll ca-profile ca-profile-name` command.

If you obtained the CA digital certificate manually through e-mail or other out-of-band mechanism, you must load it manually. To manually install a certificate in your router,

issue the **request security pki ca-certificate load ca-profile *profile_name* filename /path/*filename.cert*** command.

Generating a Private/Public Key Pair

A key pair is a critical element of a digital certificate implementation. The public key is included in the local digital certificate and the private key is used to decrypt data received from peers. To generate a private/public key pair, issue the **request security pki generate-key-pair certificate-id *certificate-id-name*** command.

Generating and Enrolling a Local Digital Certificate

You can generate and enroll a local digital certificate either online or manually. To generate and enroll a local certificate online by using SCEP, issue the **request security pki local-certificate enroll** command. To generate a local certificate request manually in the PKCS-10 format, issue the **request security pki generate-certificate-request** command.

If you create the local certificate request manually, you must also load the certificate manually. To manually install a certificate in your router, issue the **request security pki local-certificate load** command.

Applying the Local Digital Certificate to an IPsec Configuration

To activate a local digital certificate, you configure the IKE proposal to use digital certificates instead of preshared keys, reference the local certificate in the IKE policy, and identify the CA or RA in the service set. To enable the IKE proposal for digital certificates, include the **rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal *proposal-name* authentication-method]** hierarchy level. To reference the local certificate in the IKE policy, include the **local-certificate** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. To identify the CA or RA in the service set, include the **trusted-ca** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

```
[edit services]
service-set service-set-name {
  .....
  ipsec-vpn-options {
    trusted-ca ca-profile-name;
  }
}
ipsec-vpn {
  ike {
    proposal proposal-name {
      .....
      authentication-method [pre-shared-keys | rsa-signatures];
    }
    policy policy-name {
      ....
      local-certificate certificate-id-name;
    }
  }
}
```


Configuring Automatic Reenrollment of Digital Certificates

You can configure automatic reenrollment for digital certificates. This feature is by default not enabled. To configure automatic reenrollment for digital certificates, include the **auto-re-enrollment** statement at the **[edit security pki]** hierarchy level:

```
[edit]
security {
  pki {
    auto-re-enrollment {
      certificate-id certificate-name {
        ca-profile ca-profile-name;
        challenge-password password;
        re-enroll-trigger-time-percentage percentage; # Percentage of validity-period
          # (specified in certificate) when automatic
          # reenrollment should be initiated.
        re-generate-keypair;
        validity-period number-of-days;
      }
    }
  }
}
```

Monitoring and Clearing Digital Certificates

- [Monitoring Digital Certificates on page 77](#)
- [Clearing Digital Certificates on page 78](#)

Monitoring Digital Certificates

Purpose You can issue various forms of the **show security pki** command to view digital certificates and certificate requests and certificate revocation lists:

- Action**
- To display the CA digital certificate, issue the **show security pki ca-certificate ca-profile *ca-profile-name*** command.
 - To display the local digital certificate and the public key used to enroll the certificate, issue the **show security pki local-certificate certificate-id *certificate-id-name*** command.
 - To display the local certificate request in PKCS-10 format, issue the **show security pki certificate-request certificate-id *certificate-id-name*** command.
 - You can also view which digital certificates are used in IKE negotiations to establish tunnels by issuing the **show services ipsec-vpn certificates** command.
 - To display the certificate revocation list, issue the **show security pki crl ca-profile *ca-profile-name*** command.
 - To determine if a certificate is enabled for automatic-reenrollment, issue the **show security pki** command.

Clearing Digital Certificates

Purpose Variations of the **clear security pki** command enable you to delete certificates or requests and certificate revocation lists:

- Action**
- To delete the CA digital certificate, issue the **clear security pki ca-certificate ca-profile *ca-profile-name*** command.
 - To delete the local digital certificate and the associated private/public key pair, issue the **clear security pki local-certificate certificate-id *certificate-id-name*** command.
 - To delete the local certificate request, issue the **clear security pki certificate-request certificate-id *certificate-id-name*** command.
 - To clear the digital certificates that were used in IKE negotiations to establish tunnels, issue the **clear services ipsec-vpn certificates** command.
 - To delete the certificate revocation list, issue the **clear security pki crl ca-profile *ca-profile-name*** command.

- See Also**
- [Example: AS PIC IKE Dynamic SA with Digital Certificates Configuration on page 145](#)
 - *Security Services Administration Guide*
 - *Understanding Junos VPN Site Secure*

Additional IPsec Options

- [Using Filter-Based Forwarding to Select Traffic to Be Secured on page 79](#)
- [Using IPsec with a Layer 3 VPN on page 80](#)
- [Securing BGP Sessions with IPsec Transport Mode on page 82](#)
- [Securing OSPFv2 Networks with IPsec Transport Mode on page 83](#)

Using Filter-Based Forwarding to Select Traffic to Be Secured

Instead of using a firewall filter, you can also forward traffic into an IPsec security association by using a filter-based forwarding instance. First, configure the filter-based forwarding instance. Then, configure a routing table group to advertise the routes from the filter-based forwarding instance. Next, create a firewall filter for the ES PIC and reference the filter-based forwarding instance. Lastly, apply the filter and IPsec security association to the ES PIC.

```
[edit]
routing-instances {
  forwarding {
    instance-type forwarding;
    routing-options {
      static {
        route 10.10.10.0/24 next-hop 192.168.0.5;
      }
    }
  }
}
routing-options {
  rib-groups {
    group-name {
      import-rib [ inet.0 forwarding.inet.0 ];
    }
  }
}
firewall {
  family inet {
    filter filter-name {
      term term-name {
        then routing-instance instance-name;
      }
    }
  }
}
```

```

    }
  }
}
[edit]
interfaces {
  es-0/0/0 {
    unit 0 {
      tunnel {
        source source-ip-address;
        destination destination-ip-address;
      }
      family inet {
        ipsec-sa sa-name;
        filter {
          input filter-name;
        }
        address ip-address;
      }
    }
  }
}

```

Using IPsec with a Layer 3 VPN

Some key concepts to keep in mind when configuring IPsec within a VPN include the following:

- Add the inside services interface for a next-hop style service set into the routing instance by including the **interface *sp-fpc/pic/port*** statement at the **[edit routing-instances *instance-name*]** hierarchy level.
- For interface style service sets, add the interface on which you apply the service set and the services interface by including both interfaces at the **[edit routing-instances *instance-name*]** hierarchy level.
- To define a routing instance for the local gateway within the service set, include the **routing-instance *instance-name*** option at the **[edit services service-set *service-set-name* ipsec-vpn-options local-gateway *address*]** hierarchy level.

The following configuration for an AS PIC on a provider edge (PE) router demonstrates the use of next-hop service sets with an IKE dynamic SA in a VPN routing and forwarding (VRF) routing instance.

```

[edit]
interfaces {
  so-0/0/0 {
    description "Interface connected to the customer edge (CE) router";
    unit 0 {
      family inet {
        address 10.6.6.6/32;
      }
    }
  }
}

```

```

so-2/2/0 {
  description "Source IPsec tunnel interface to the network core";
  unit 0 {
    family inet {
      address 10.10.1.1/30;
    }
  }
}
sp-3/1/0 {
  description "AS PIC interface";
  unit 0 {
    family inet {
      address 10.7.7.7/32;
    }
  }
  unit 1 {
    family inet;
    service-domain inside;
  }
  unit 2 {
    family inet;
    service-domain outside;
  }
}
}
policy-options {
  policy-statement vpn-export-policy {
    then {
      community add community-name;
      accept;
    }
  }
  policy-statement vpn-import-policy {
    term term-name {
      from community community-name;
      then accept;
    }
  }
  community community-name members target:100:20;
}
routing-instances {
  vrf {
    instance-type vrf;
    interface sp-3/1/0.1; # Inside sp interface.
    interface so-0/0/0.0; # Interface that connects to the CE router.
    route-distinguisher route-distinguisher;
    vrf-import vpn-import-policy;
    vrf-export vpn-export-policy;
    routing-options {
      static {
        route ip-address/prefix next-hop so-0/0/0.0; # Routes for the CE router.
        route ip-address/prefix next-hop sp-3/1/0.1; # Routes for IPsec.
      }
    }
  }
}

```

```

}
services {
  service-set service-set-name {
    next-hop-service {
      inside-service-interface sp-3/1/0.1;
      outside-service-interface sp-3/1/0.2;
    }
    ipsec-vpn-options {
      local-gateway 10.10.1.1;
    }
    ipsec-vpn-rules rule-name;
  }
  ipsec-vpn {
    rule rule-name {
      term term-name {
        from {
          source-address {
            source-ip-address;
          }
        }
        then {
          remote-gateway 10.10.1.2;
          dynamic {
            ike-policy ike-policy-name;
          }
        }
      }
    }
    match-direction direction;
  }
  ike {
    policy ike-policy-name {
      pre-shared-key ascii-text preshared-key;
    }
  }
}

```

For more information on VRF routing instances, see the *Junos VPNs Configuration Guide*.
 For more information on next-hop service sets, see the *Junos Services Interfaces Configuration Guide*.

Securing BGP Sessions with IPsec Transport Mode

For the ES PIC, you can use IPsec to secure BGP sessions between Routing Engines in M Series and T Series platforms. To configure, create a transport mode security association and apply the SA to the BGP configuration by including the **ipsec-sa** statement at the **[edit protocols bgp group group-name]** hierarchy level.

```

[edit]
protocols {
  bgp {
    group group-name {
      local-address ip-address;
    }
  }
}

```

```

    export export-policy;
    peer-as as-number;
    ipsec-sa sa-name;
    neighbor peer-ip-address;
  }
}

```

Related Documentation • [IPsec Modes on page 61](#)

Securing OSPFv2 Networks with IPsec Transport Mode

By default, you can configure MD5 or simple text password-based authentication over OSPFv2 links. In addition to these basic authentications, the Junos OS supports OSPFv2 with a security authentication header (AH), Encapsulating Security Payload (ESP), or an IPsec protocol bundle that supports both AH and ESP. You can configure IPsec over OSPFv2 using transport mode security associations on physical, sham, or virtual links.

Because the Junos OS supports only bidirectional security associations over OSPFv2, OSPFv2 peers must be configured with the same IPsec security association. Configuring OSPFv2 peers with different security associations or with dynamic IKE will prevent adjacencies from being established. In addition, you must configure identical security associations for sham links with the same remote endpoint address, for virtual links with the same remote endpoint address, for all neighbors on OSPF nonbroadcast multiaccess (NBMA) or point-to-multipoint links, and for every subnet that is part of a broadcast link.

To create a manual bidirectional security association, include the **security-association** *security-association-name* statement at the `[edit security ipsec]` hierarchy level:

```

[edit]
security {
  ipsec {
    security-association security-association name {
      mode transport;
      manual {
        direction bidirectional {
          protocol (ah | esp | bundle);
          spi spi--value;
          authentication {
            algorithm (hmac-md5-96 | hmac-sha1-96);
            key (ascii-text key | hexadecimal key);
          }
        }
      }
    }
  }
}

```

To configure IPsec on an OSPFv2 interface, create a transport mode security association and include the `ipsec-sa name` statement at the `[edit protocols ospf area area-id]` hierarchy level:

```
[edit]
protocols {
  ospf {
    area area-id {
      interface interface-name {
        ipsec-sa sa-name;
      }
      virtual-link neighbor-id a.b.c.d transit-area x.x.x.x {
        ipsec-sa sa-name;
      }
      sham-link-remote {
        ipsec-sa sa-name;
      }
    }
  }
}
```

To verify your configuration, enter the `show ospf interface detail` command. This command gives detailed information about the `ospfv2` interface and displays the interface's security association at the bottom of the output. In the example below, the security association configured on this router is `sa1`.

```
user@router> show ospf interface detail
```

```
Interface          State      Area      DR ID      BDR ID Nbrs
fe-0/0/1.0         BDR       0.0.0.0    192.168.37.12 10.255.245.215 1
Type LAN, address 192.168.37.11, Mask 255.255.255.248, MTU 4460, Cost 40
DR addr 192.168.37.12, BDR addr 192.168.37.11, Adj count 1, Priority 128
Hello 10, Dead 40, ReXmit 5, Not Stub
t1-0/2/1.0         PtToPt    0.0.0.0    0.0.0.0     0.0.0.0 0
Type P2P, Address 0.0.0.0, Mask 0.0.0.0, MTU 1500, Cost 2604
Adj count 0
Hello 10, Dead 40, ReXmit 5, Not Stub
Auth type: MD5, Active key ID 3, Start time 2002 Nov 19 10:00:00 PST
IPsec SA Name: sa1
```

Related Documentation

- [IPSec Modes on page 61](#)

Configuring IPsec Dynamic Endpoints

- [Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels on page 85](#)
- [Configuring the Service Set for IPsec Dynamic Endpoint Tunnels on page 86](#)
- [Configuring the Interface Identifier for IPsec Dynamic Endpoint Tunnels on page 87](#)
- [Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels on page 87](#)

Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels

You can configure only one tunnel profile per service set for all dynamic peers. The configured preshared key in the profile is used for IKE authentication of all dynamic peers terminating in that service set.

The IKE tunnel profile specifies all the information needed to complete the IKE negotiation. For more information on access profiles, see the *Junos System Basics Configuration Guide*.

```
[edit access]
profile profile-name {
  client * {
    ike {
      allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
      }
      pre-shared-key ([ ascii-text key-string ] | [ hexadecimal key-string ]);
      interface-id string-value;
      ipsec-policy ipsec-policy;
    }
  }
}
```



NOTE: For dynamic peers, the Junos OS supports only IKE main mode with the preshared key method of authentication. In this mode, an IPv4 or IPv6 address is used to identify a tunnel peer to get the preshared key information. The client value * (wildcard) means that the configuration within this profile is valid for all dynamic peers terminating within the service set accessing this profile.

The following statements are the parts of the IKE profile:

- **allowed-proxy-pair**—During phase 2 IKE negotiation, the remote peer supplies its network address (**remote**) and its peer's network address (**local**). Since multiple dynamic tunnels are authenticated through the same mechanism, this statement must include the list of possible combinations. If the dynamic peer does not present a valid combination, the phase 2 IKE negotiation fails.

By default, remote 0.0.0.0/0 local 0.0.0.0/0 is used if no values are configured.

- **pre-shared-key**—Mandatory key used to authenticate the dynamic peer during IKE phase 1 negotiation. This key must be configured on both ends of the tunnel and distributed through an out-of-band secure mechanism. You can configure the key value either in **hexadecimal** or **ascii-text** format.
- **interface-id**—Interface identifier, a mandatory attribute used to derive the logical service interface information for the session.
- **ipsec-policy**—Name of the IPsec policy that defines the IPsec policy information for the session. You define the IPsec policy at the **[edit services ipsec-vpn ipsec policy policy-name]** hierarchy level. If no policy is set, any policy proposed by the dynamic peer is accepted.

Configuring the Service Set for IPsec Dynamic Endpoint Tunnels

To complete a dynamic endpoint tunnel configuration, you need to reference the IKE access profile configured at the **[edit access]** hierarchy level in the service set. To do this, include the **ike-access-profile** statement at the **[edit services service-set name ipsec-vpn-options]** hierarchy level:

```
[edit services]
service-set name {
  next-hop-service {
    inside-service-interface interface-name;
    outside-service-interface interface-name;
  }
  ipsec-vpn-options {
    local-gateway address;
    ike-access-profile profile-name;
  }
}
```

You can reference only one access profile in each service set. This profile is used to negotiate IKE and IPsec security associations with dynamic peers only.



NOTE: If you configure an IKE access profile in a service set, no other service set can share the same **local-gateway** address.

Configuring the Interface Identifier for IPsec Dynamic Endpoint Tunnels

You can configure an interface identifier for a group of dynamic peers, which specifies which adaptive services logical interface(s) take part in the dynamic IPsec negotiation. By assigning the same interface identifier to multiple logical interfaces, you can create a pool of interfaces for this purpose. To configure, include the **ipsec-interface-id** statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces sp-fpc/pic/port]
unit logical-unit-number {
  dial-options {
    ipsec-interface-id identifier;
    (shared | dedicated);
  }
}
```

Specifying the interface identifier in the **dial-options** statement makes this logical interface part of the pool identified by the IPsec interface identifier.



NOTE: Only one interface identifier can be specified at a time. You can include the **ipsec-interface-id** statement or the **l2tp-interface-id** statement, but not both simultaneously.

The **shared** statement enables one logical interface to be shared across multiple tunnels. The **dedicated** statement specifies that the logical interface is associated with a single tunnel, which is necessary when you are configuring an IPsec link-type tunnel. You must include the **dedicated** statement when you specify an **ipsec-interface-id** value.

Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels

- [Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels on page 87](#)
- [Configuring the Service Set for IPsec Dynamic Endpoint Tunnels on page 88](#)
- [Configuring the Interface Identifier for IPsec Dynamic Endpoint Tunnels on page 89](#)
- [Configuring Multiple Routed Tunnels in a Single Next-Hop Service Set on page 89](#)

Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels

You can configure only one tunnel profile per service set for all dynamic peers. The configured preshared key in the profile is used for IKE authentication of all dynamic peers terminating in that service set.

The IKE tunnel profile specifies all the information needed to complete the IKE negotiation. For more information on access profiles, see the *Junos System Basics Configuration Guide*.

```
[edit access]
profile profile-name {
  client * {
```

```

ike {
  allowed-proxy-pair {
    remote remote-proxy-address local local-proxy-address;
  }
  pre-shared-key ([ ascii-text key-string ] | [hexadecimal key-string ]);
  interface-id string-value;
  ipsec-policy ipsec-policy;
}
}

```



NOTE: For dynamic peers, the Junos OS supports only IKE main mode with the preshared key method of authentication. In this mode, an IPv4 or IPv6 address is used to identify a tunnel peer to get the preshared key information. The client value * (wildcard) means that the configuration within this profile is valid for all dynamic peers terminating within the service set accessing this profile.

The following statements are the parts of the IKE profile:

- **allowed-proxy-pair**—During phase 2 IKE negotiation, the remote peer supplies its network address (**remote**) and its peer's network address (**local**). Since multiple dynamic tunnels are authenticated through the same mechanism, this statement must include the list of possible combinations. If the dynamic peer does not present a valid combination, the phase 2 IKE negotiation fails.

By default, remote 0.0.0.0/0 local 0.0.0.0/0 is used if no values are configured.

- **pre-shared-key**—Mandatory key used to authenticate the dynamic peer during IKE phase 1 negotiation. This key must be configured on both ends of the tunnel and distributed through an out-of-band secure mechanism. You can configure the key value either in **hexadecimal** or **ascii-text** format.
- **interface-id**—Interface identifier, a mandatory attribute used to derive the logical service interface information for the session.
- **ipsec-policy**—Name of the IPsec policy that defines the IPsec policy information for the session. You define the IPsec policy at the **[edit services ipsec-vpn ipsec policy *policy-name*]** hierarchy level. If no policy is set, any policy proposed by the dynamic peer is accepted.

Configuring the Service Set for IPsec Dynamic Endpoint Tunnels

To complete a dynamic endpoint tunnel configuration, you need to reference the IKE access profile configured at the **[edit access]** hierarchy level in the service set. To do this, include the **ike-access-profile** statement at the **[edit services service-set *name* ipsec-vpn-options]** hierarchy level:

```

[edit services]
service-set name {

```

```

next-hop-service {
  inside-service-interface interface-name;
  outside-service-interface interface-name;
}
ipsec-vpn-options {
  local-gateway address;
  ike-access-profile profile-name;
}
}

```

You can reference only one access profile in each service set. This profile is used to negotiate IKE and IPsec security associations with dynamic peers only.



NOTE: If you configure an IKE access profile in a service set, no other service set can share the same **local-gateway** address.

Configuring the Interface Identifier for IPsec Dynamic Endpoint Tunnels

You can configure an interface identifier for a group of dynamic peers, which specifies which adaptive services logical interface(s) take part in the dynamic IPsec negotiation. By assigning the same interface identifier to multiple logical interfaces, you can create a pool of interfaces for this purpose. To configure, include the **ipsec-interface-id** statement at the [edit interfaces *interface-name*] hierarchy level:

```

[edit interfaces sp-fpc/pic/port]
unit logical-unit-number {
  dial-options {
    ipsec-interface-id identifier;
    (shared | dedicated);
  }
}

```

Specifying the interface identifier in the **dial-options** statement makes this logical interface part of the pool identified by the IPsec interface identifier.



NOTE: Only one interface identifier can be specified at a time. You can include the **ipsec-interface-id** statement or the **l2tp-interface-id** statement, but not both simultaneously.

The **shared** statement enables one logical interface to be shared across multiple tunnels. The **dedicated** statement specifies that the logical interface is associated with a single tunnel, which is necessary when you are configuring an IPsec link-type tunnel. You must include the **dedicated** statement when you specify an **ipsec-interface-id** value.

Configuring Multiple Routed Tunnels in a Single Next-Hop Service Set

You can optionally configure several routed IPsec tunnels within a single next-hop service set. To do so, start by establishing multiple services interfaces as inside interfaces by

including the **service-domain inside** statement at the **[edit interfaces sp-fpc/pic/port unit logical-unit-number]** hierarchy level. Then, include the **ipsec-inside-interface** statement at the **[edit services ipsec-vpn rule rule-name term term-name from]** hierarchy level.



NOTE: The full IPsec and IKE proposals and policies are not shown in the following example for the sake of brevity.

```
[edit]
interfaces {
  sp-3/3/0 {
    unit 3 {
      family inet;
      service-domain inside;
    }
    unit 4 {
      family inet;
      service-domain outside;
    }
    unit 5 {
      family inet;
      service-domain inside;
    }
  }
}
services {
  service-set link_type_ss_1 {
    next-hop-service {
      inside-service-interface sp-3/3/0.3;
      outside-service-interface sp-3/3/0.4;
    }
    ipsec-vpn-options {
      local-gateway 10.8.7.2;
    }
    ipsec-vpn-rules link_rule_1;
  }
  ipsec-vpn {
    rule link_rule_1 {
      term 1 {
        from {
          ipsec-inside-interface sp-3/3/0.3;
        }
        then {
          remote-gateway 10.10.7.3;
          backup-remote-gateway 10.8.7.1;
          dynamic {
            ike-policy main_mode_ike_policy;
            ipsec-policy dynamic_ipsec_policy;
          }
        }
      }
      term 2 {
        from {
```

```

    ipsec-inside-interface sp-3/3/0.5;
  }
  then {
    remote-gateway 10.12.7.5;
    dynamic {
      ike-policy main_mode_ike_policy;
      ipsec-policy dynamic_ipsec_policy;
    }
  }
}
match-direction input;
}
}
}

```

To confirm that your configuration is working, issue the **show services ipsec-vpn ipsec security-associations** command. Notice that each IPsec inside interface that you assigned to each IPsec tunnel is included in the output of this command.

```
user@router> show services ipsec-vpn ipsec security-associations
```

```
Service set: link_type_ss_1
```

```

Rule: link_rule_1, Term: 1, Tunnel index: 1
Local gateway: 10.8.7.2, Remote gateway: 10.8.7.1
IPSec inside interface: sp-3/3/0.3
  Direction SPI      AUX-SPI    Mode      Type      Protocol
  inbound  3216392497  0         tunnel    dynamic   ESP
  outbound 398917249  0         tunnel    dynamic   ESP

Rule: link_rule_1, Term: 2, Tunnel index: 2
Local gateway: 10.8.7.2, Remote gateway: 10.12.7.5
IPSec inside interface: sp-3/3/0.5
  Direction SPI      AUX-SPI    Mode      Type      Protocol
  inbound  762146783  0         tunnel    dynamic   ESP
  outbound 319191515  0         tunnel    dynamic   ESP

```

See Also • [Configuring IKE Dynamic SAs on page 66](#)

CHAPTER 8

Additional ES and AS PIC Configuration Examples

- [Example: ES PIC Manual SA Configuration on page 93](#)
- [Example: AS PIC Manual SA Configuration on page 102](#)
- [Example: ES PIC IKE Dynamic SA Configuration on page 111](#)
- [Example: AS PIC IKE Dynamic SA Configuration on page 122](#)
- [Example: IKE Dynamic SA Between an AS PIC and an ES PIC Configuration on page 131](#)
- [Example: AS PIC IKE Dynamic SA with Digital Certificates Configuration on page 145](#)
- [Example: Dynamic Endpoint Tunneling Configuration on page 164](#)

Example: ES PIC Manual SA Configuration

Figure 4: ES PIC Manual SA Topology Diagram

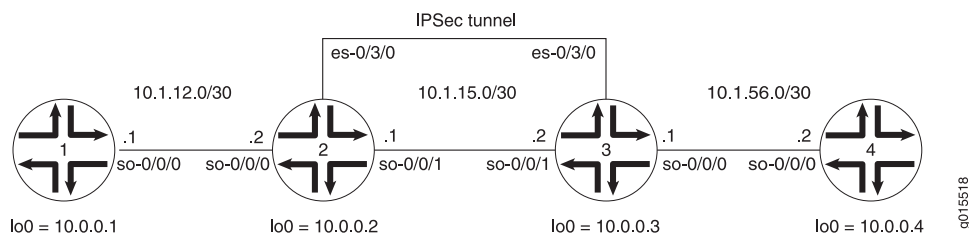


Figure 4 on page 93 shows an IPSec topology containing a group of four routers. Routers 2 and 3 establish an IPSec tunnel using an ES PIC and manual SA settings. Routers 1 and 4 provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

```
Router 1 [edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
}
```

```

}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.1/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.1;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}
}

```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional manual SA called **sa-manual** at the **[edit security ipsec security-association]** hierarchy level. Use AH for the protocol, **400** for the SPI, HMAC-MD5-96 for authentication, and a 32-bit hexadecimal authentication key for the MD5 authentication key. (For more information about key length, see [Table 5 on page 33](#).) Because you are using AH, there is no need to configure encryption.

To direct traffic into the ES PIC and the IPsec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 1 destined for Router 4, whereas the **es-return** filter matches the return path from Router 4 to Router 1. Apply the **es-traffic** filter to the **so-0/0/0** interface; then apply both the **es-return** filter and the **sa-manual** SA to the **es-0/3/0** interface.

Router 2

```

[edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPsec tunnel here.
        }
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.1/30;
      }
    }
  }
}

```

```

    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.1;
        destination 10.1.15.2;
      }
      family inet {
        ipsec-sa sa-manual; # Apply the manual SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.2/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
security {
  ipsec {
    security-association sa-manual { # Define the manual SA specifications here.
      mode tunnel;
      manual {
        direction bidirectional {
          protocol ah;
          spi 400;
          authentication {
            algorithm hmac-md5-96;
            key hexadecimal "$ABC123";
          }
        }
      }
    }
  }
}
}

```

```
# The 32-bit unencrypted hexadecimal key is abcdef01abcdef01abcdef01abcdef01.
firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPsec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.12.0/24;
        }
        destination-address {
          10.1.56.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-manual;
      }
    }
    term other {
      then accept;
    }
  }
  filter es-return { # Define a filter that matches return IPsec traffic here.
    term return {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then accept;
    }
  }
}
```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional manual SA called **sa-manual** at the **[edit security ipsec security-association]** hierarchy level. Use the exact same specifications that you used for the SA on Router 2: AH for the protocol, **400** for the SPI, HMAC-MD5-96 for authentication, and a 32-bit hexadecimal authentication key of **abcdef01abcdef01abcdef01abcdef01** for the MD5 authentication key. (For more information about authentication key length, see [Table 5 on page 33](#).) Because you are using AH, there is no need to configure an encryption algorithm.

To direct traffic into the ES PIC and the IPsec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 4 destined for Router 1, whereas the **es-return** filter matches the return path from Router 1 to Router 4. Apply the **es-traffic** filter to the **so-0/0/0** interface; then apply both the **es-return** filter and the **sa-manual** SA to the **es-0/3/0** interface.

Router 3

```
[edit]
interfaces {
```

```
so-0/0/0 {
  description "To R4 so-0/0/0";
  unit 0 {
    family inet {
      filter {
        input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
      }
      address 10.1.56.1/30;
    }
  }
}
so-0/0/1 {
  description "To R2 so-0/0/1";
  unit 0 {
    family inet {
      address 10.1.15.2/30;
    }
  }
}
es-0/3/0 {
  unit 0 {
    tunnel { # Specify the IPSec tunnel endpoints here.
      source 10.1.15.2;
      destination 10.1.15.1;
    }
    family inet {
      ipsec-sa sa-manual; # Apply the manual SA here.
      filter {
        input es-return; # Apply the filter that matches return IPSec traffic here.
      }
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.3/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
}
security {
  ipsec {
```

```
security-association sa-manual { # Define the manual SA specifications here.
  mode tunnel;
  manual {
    direction bidirectional {
      protocol ah;
      spi 400;
      authentication {
        algorithm hmac-md5-96;
        key hexadecimal "$ABC123";
      }
    }
  }
}
```

```
## The 32-bit unencrypted hexadecimal key is abcdef01abcdef01abcdef01abcdef01.
firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-manual;
      }
    }
    term other {
      then accept;
    }
  }
  filter es-return { # Define a filter that matches return IPSec traffic here.
    term return {
      from {
        source-address {
          10.1.12.0/24;
        }
        destination-address {
          10.1.56.0/24;
        }
      }
      then accept;
    }
  }
}
```

On Router 4, provide basic OSPF connectivity to Router 3.

```
Router 4 [edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.ping
    }
  }
}
```

Verifying Your Work

To verify proper operation of a manual IPsec SA on the ES PIC, use the following commands:

- **ping**
- **show ipsec security-associations (detail)**
- **traceroute**

The following sections show the output of these commands used with the configuration example:

- [Router 1 on page 100](#)
- [Router 2 on page 100](#)
- [Router 3 on page 101](#)
- [Router 4 on page 102](#)

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface of Router 4 to send traffic across the IPsec tunnel.

```
user@R1> ping 10.1.56.2

PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=253 time=0.939 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=253 time=0.886 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=253 time=0.826 ms
^C
--- 10.1.56.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.826/0.884/0.939/0.046 ms
```

You can also issue the **traceroute** command to verify that traffic to **10.1.56.2** travels over the IPsec tunnel between Router 2 and Router 3. Notice that the second hop does not reference **10.1.15.2**—the physical interface on Router 3. Instead, the loopback address of **10.0.0.3** on Router 3 appears as the second hop. This indicates that the IPsec tunnel is operating correctly.

```
user@R1> traceroute 10.1.56.2

traceroute to 10.1.56.2 (10.1.56.2), 30 hops max, 40 byte packets
 1  10.1.12.1 (10.1.12.1)  0.655 ms  0.549 ms  0.508 ms
 2  10.0.0.3 (10.0.0.3)  0.833 ms  0.786 ms  0.757 ms
 3  10.1.56.2 (10.1.56.2)  0.808 ms  0.741 ms  0.716 ms
```

Router 2

Another way to verify that matched traffic is being diverted to the bidirectional IPsec tunnel is to view the firewall filter counter. After you issue the **ping** command from Router 1 (three packets), the **es-traffic** firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic

Filter: es-traffic
Counters:
Name                               Bytes      Packets
-----
ipsec-tunnel                        252         3
```

After you issue the **ping** command from both Router 1 (three packets) and Router 4 (two packets), the **es-traffic** firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic

Filter: es-traffic
Counters:
Name                               Bytes      Packets
-----
ipsec-tunnel                       420         5
```


To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the SA contains the settings you specified, such as AH for the protocol and HMAC-MD5-96 for the authentication algorithm.

```
user@R2> show ipsec security-associations detail
```

```
Security association: sa-manual, Interface family: Up
```

```
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Direction: inbound, SPI: 400, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Anti-replay service: Disabled
```

```
Direction: outbound, SPI: 400, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPsec tunnel. After you issue the **ping** command from Router 1 (three packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
```

```
Filter: es-traffic
```

```
Counters:
```

Name	Bytes	Packets
ipsec-tunnel	252	3

After you issue the **ping** command from both Router 1 (three packets) and Router 4 (two packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
```

```
Filter: es-traffic
```

```
Counters:
```

Name	Bytes	Packets
ipsec-tunnel	420	5

To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ipsec security-associations detail
```

```
Security association: sa-manual, Interface family: Up
```

```
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```

Direction: inbound, SPI: 400, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Anti-replay service: Disabled

Direction: outbound, SPI: 400, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Anti-replay service: Disabled

```

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface of Router 1 to send traffic across the IPsec tunnel.

```

user@R4> ping 10.1.12.2

PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=253 time=0.937 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=253 time=0.872 ms
^C
--- 10.1.12.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.872/0.905/0.937/0.032 ms

```

You can also issue the **traceroute** command to verify that traffic to **10.1.12.2** travels over the IPsec tunnel between Router 3 and Router 2. Notice that the second hop does not reference **10.1.15.1**—the physical interface on Router 2. Instead, the loopback address of **10.0.0.2** on Router 2 appears as the second hop. This indicates that the IPsec tunnel is operating correctly.

```

user@R4> traceroute 10.1.12.2

traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1  10.1.56.1 (10.1.56.1)  0.670 ms  0.589 ms  0.548 ms
 2  10.0.0.2 (10.0.0.2)  0.815 ms  0.791 ms  0.763 ms
 3  10.1.12.2 (10.1.12.2)  0.798 ms  0.741 ms  0.714 ms

```

Example: AS PIC Manual SA Configuration

Figure 5: AS PIC Manual SA Topology Diagram

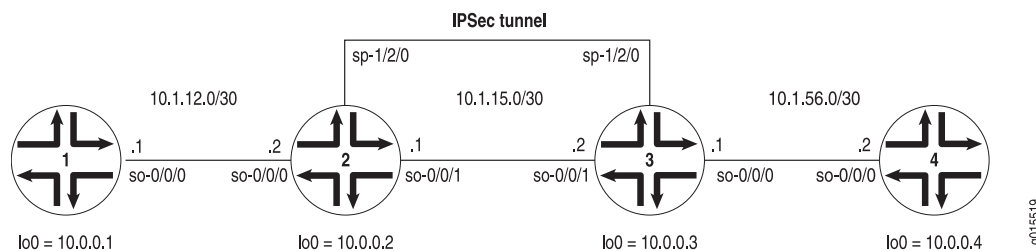


Figure 5 on page 102 shows a similar IPsec topology to the one used in the ES PIC manual SA example. The difference is that Routers 2 and 3 establish an IPsec tunnel using an

AS PIC and use slightly modified manual SA settings. Routers 1 and 4 again provide basic connectivity and are used to verify that the IPsec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

```
Router 1 [edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.1/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.1;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}
```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional manual SA in a rule called rule-manual-SA-BiEspshades at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called service-set-manual-BiEspshades at the **[edit services service-set]** hierarchy level.

Configure all specifications for your manual SA. Use ESP for the protocol, **261** for the SPI, HMAC-SHA1-96 for authentication, DES-CBC for encryption, a 20-bit ASCII authentication key for the SHA-1 authentication key, and an 8-bit ASCII encryption key for the DES-CBC authentication key. (For more information about key lengths, see [Table 5 on page 33](#).)

To direct traffic into the AS PIC and the IPsec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPsec inside interface into the OSPF configuration.

```
Router 2 [edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
```

```
unit 0 {
  family inet {
    address 10.1.12.1/30;
  }
}
}
so-0/0/1 {
  description "To R3 so-0/0/1";
  unit 0 {
    family inet {
      address 10.1.15.1/30;
    }
  }
}
sp-1/2/0 {
  services-options {
    syslog {
      host local {
        services info;
      }
    }
  }
  unit 0 {
    family inet {
    }
  }
  unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
    family inet;
    service-domain inside;
  }
  unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
    family inet;
    service-domain outside;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.2/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
      interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
    }
  }
}
}
services {
```

```

service-set service-set-manual-BiEspshades { # Define your service set here.
  next-hop-service { # Required for dynamic routing protocols such as OSPF.
    inside-service-interface sp-1/2/0.1;
    outside-service-interface sp-1/2/0.2;
  }
  ipsec-vpn-options {
    local-gateway 10.1.15.1; # Specify the local IP address of the IPsec tunnel.
  }
  ipsec-vpn-rules rule-manual-SA-BiEspshades; # Reference the IPsec rule here.
}
ipsec-vpn {
  rule rule-manual-SA-BiEspshades { # Define your IPsec VPN rule here.
    term term-manual-SA-BiEspshades {
      then {
        remote-gateway 10.1.15.2; # The remote IP address of the IPsec tunnel.
        manual { # Define the manual SA specifications here.
          direction bidirectional {
            protocol esp;
            spi 261;
            authentication {
              algorithm hmac-sha1-96;
              key ascii-text "$ABC123";
              ## The unencrypted key is juniperjuniperjunipe (20 characters for
              HMAC-SHA-1-96).
            }
            encryption {
              algorithm des-cbc;
              key ascii-text "$ABC123";
              ## The unencrypted key is juniperj (8 characters for DES-CBC).
            }
          }
        }
      }
    }
  }
  match-direction input; # Correct match direction for next-hop service sets.
}
}
}
security {
  pki {
    auto-re-enrollment {
      certificate-id certificate-name {
        ca-profile ca-profile-name;
        challenge-password password;
        re-enroll-trigger-time-percentage percentage; #Percentage of validity-period
        # (specified in certificate) when automatic
        # reenrollment should be initiated.
        re-generate-keypair;
        validity-period number-of-days;
      }
    }
  }
}

```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional manual SA in a rule called rule-manual-SA-BiEspshades at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called service-set-manual-BiEspshades at the **[edit services service-set]** hierarchy level.

Configure the same specifications for your manual SA that you specified on Router 2. Use ESP for the protocol, **261** for the SPI, HMAC-SHA1-96 for authentication, DES-CBC for encryption, a 20-bit ASCII authentication key for the SHA-1 authentication key, and an 8-bit ASCII encryption key for the DES-CBC authentication key. (For more information about key lengths, see [Table 5 on page 33](#).)

To direct traffic into the AS PIC and the IPsec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPsec inside interface into the OSPF configuration.

Router 3

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.2/30;
      }
    }
  }
  sp-1/2/0 {
    services-options {
      syslog {
        host local {
          services info;
        }
      }
    }
    unit 0 {
      family inet {
      }
    }
    unit 1 { # sp-1/2/0.1 is the IPsec inside interface.
      family inet;
      service-domain inside;
    }
    unit 2 { # sp-1/2/0.2 is the IPsec outside interface.
      family inet;
      service-domain outside;
    }
  }
}
```

```

lo0 {
  unit 0 {
    family inet {
      address 10.0.0.3/32;
    }
  }
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
      interface sp-1/2/0.1; # This sends OSPF traffic over the IPsec tunnel.
    }
  }
}
services {
  service-set service-set-manual-BiEspshades { # Define your service set here.
    next-hop-service { # Required for dynamic routing protocols such as OSPF.
      inside-service-interface sp-1/2/0.1;
      outside-service-interface sp-1/2/0.2;
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.2; # Specify the local IP address of the IPsec tunnel.
    }
    ipsec-vpn-rules rule-manual-SA-BiEspshades; # Reference the IPsec rule here.
  }
  ipsec-vpn {
    rule rule-manual-SA-BiEspshades { # Define your IPsec VPN rule here.
      term term-manual-SA-BiEspshades {
        then {
          remote-gateway 10.1.15.1; # The remote IP address of the IPsec tunnel.
          manual { # Define the manual SA specifications here.
            direction bidirectional {
              protocol esp;
              spi 261;
              authentication {
                algorithm hmac-sha1-96;
                key ascii-text "$ABC123";
                ## The unencrypted key is juniperjuniperjunipe (20 characters for
                HMAC-SHA-1-96).
              }
              encryption {
                algorithm des-cbc;
                key ascii-text "$ABC123";
                ## The unencrypted key is juniperj (8 characters for DES-CBC).
              }
            }
          }
        }
      }
    }
  }
}

```

```
        match-direction input; # Specify in which direction the rule should match.
    }
}
}
```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}
```

Verifying Your Work

To verify proper operation of a manual IPsec SA on the AS PIC, use the following commands:

- **ping**
- **show services ipsec-vpn ipsec security-associations (detail)**
- **show services ipsec-vpn ipsec statistics**

The following sections show the output of these commands used with the configuration example:

- [Router 1 on page 109](#)
- [Router 2 on page 109](#)
- [Router 3 on page 110](#)

Router 1

On Router 1, issue a **ping** command to the **lo0** interface on Router 4 to send traffic across the IPsec tunnel.

```
user@R1> ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4): 56 data bytes
64 bytes from 10.0.0.4: icmp_seq=0 ttl=254 time=1.375 ms
64 bytes from 10.0.0.4: icmp_seq=1 ttl=254 time=18.375 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=254 time=1.120 ms
^C
--- 10.0.0.4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.120/6.957/18.375/8.075 ms
```

Router 2

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the settings you specified, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-manual-BiEspshades
Rule: rule-manual-SA-BiEspshades, Term: term-manual-SA-BiEspshades,
Tunnel index: 1
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=10.0.0.0/8)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

Direction: inbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled

Direction: outbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled
```

To verify that traffic is traveling over the bidirectional IPsec tunnel, issue the **show services ipsec-vpn statistics** command:

```
user@R2> show services ipsec-vpn ipsec statistics
```

```
PIC: sp-1/2/0, Service set: service-set-manual-BiEspshades
```

ESP Statistics:

```
Encrypted bytes:      1616
Decrypted bytes:      1560
Encrypted packets:    20
Decrypted packets:    19
```

AH Statistics:

```
Input bytes:          0
Output bytes:          0
Input packets:         0
Output packets:        0
```

Errors:

```
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

Router 3

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: service-set-manual-BiEspshades
```

```
Rule: rule-manual-SA-BiEspshades, Term: term-manual-SA-BiEspshades,
Tunnel index: 1
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.0.0.0/8)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Direction: inbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled
```

```
Direction: outbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled
```

To verify that traffic is traveling over the bidirectional IPsec tunnel, issue the **show services ipsec-vpn statistics** command:

```
user@R3> show services ipsec-vpn ipsec statistics
```

```
PIC: sp-1/2/0, Service set: service-set-manual-BiEspshades
```

ESP Statistics:

```
Encrypted bytes:      1560
Decrypted bytes:      1616
Encrypted packets:    19
Decrypted packets:    20
```

AH Statistics:

```
Input bytes:          0
Output bytes:          0
```

```

Input packets:          0
Output packets:         0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0

```

Example: ES PIC IKE Dynamic SA Configuration

Figure 6: ES PIC IKE Dynamic SA Topology Diagram

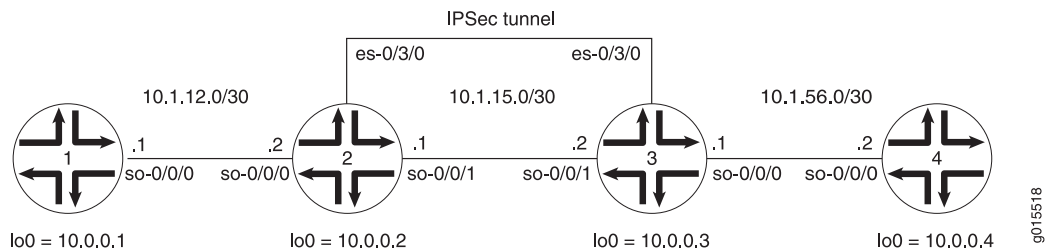


Figure 6 on page 111 shows the same IPSec topology as seen in the ES PIC manual SA example. However, this time the configuration requires Routers 2 and 3 to establish an IPSec tunnel using an IKE dynamic SA, enhanced authentication, and stronger encryption. Routers 1 and 4 continue to provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

```

Router 1 [edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.1/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.1;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
    }
  }
}

```

```

    interface lo0.0;
  }
}

```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA called **sa-dynamic** at the **[edit security ipsec security-association]** hierarchy level. For your IKE policy and proposal, use preshared keys for the authentication method, SHA-1 for the authentication algorithm, 3DES-CBC for encryption, group 2 for the Diffie-Hellman group, main mode, 3600 seconds for the lifetime, and a preshared key of **juniper** for the initial IKE negotiation. For your IPSec policy and proposal, use ESP for the protocol, HMAC-SHA1-96 for authentication, 3DES-CBC for encryption, 28800 seconds for the lifetime, and group 2 for the PFS group.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 1 destined for Router 4, whereas the **es-return** filter matches the return path from Router 4 to Router 1. Apply the **es-traffic** filter to the **so-0/0/0** interface, and then apply both the **es-return** filter and the **sa-dynamic** SA to the **es-0/3/0** interface.

Router 2

```

[edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.1/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.1;
        destination 10.1.15.2;
      }
      family inet {
        ipsec-sa sa-dynamic; # Apply the dynamic SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
}

```

```

    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.2/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
security {
  ipsec {
    proposal es-ipsec-proposal { # Define your IPSec proposal specifications here.
      protocol esp;
      authentication-algorithm hmac-sha1-96;
      encryption-algorithm 3des-cbc;
      lifetime-seconds 28800;
    }
    policy es-ipsec-policy { # Define your IPSec policy specifications here.
      perfect-forward-secrecy {
        keys group2;
      }
      proposals es-ipsec-proposal; # Reference the IPSec proposal here.
    }
    security-association sa-dynamic { # Define your dynamic SA here.
      mode tunnel;
      dynamic {
        ipsec-policy es-ipsec-policy; # Reference the IPSec policy here.
      }
    }
  }
}
ike {
  proposal es-ike-proposal { # Define your IKE proposal specifications here.
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 3600;
  }
  policy 10.1.15.2 { # Define your IKE policy specifications here.
    mode main;
    proposals es-ike-proposal; # Reference the IKE proposal here.
  }
}

```

```

    pre-shared-key ascii-text "$ABC123";
    ## The unencrypted preshared key for this example is juniper.
  }
}
firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.12.0/24;
        }
        destination-address {
          10.1.56.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-dynamic;
      }
    }
    term other {
      then accept;
    }
  }
  filter es-return { # Define a filter that matches return IPSec traffic here.
    term return {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then accept;
    }
  }
}

```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA called **sa-dynamic** at the **[edit security ipsec security-association]** hierarchy level. Use the same policies and proposals that you used on Router 2.

For your IKE policy and proposal, use preshared keys for the authentication method, SHA-1 for the authentication algorithm, 3DES-CBC for encryption, group 2 for the Diffie-Hellman group, main mode, 3600 seconds for the lifetime, and a preshared key of **juniper** for the initial IKE negotiation. For your IPSec policy and proposal, use ESP for the protocol, HMAC-SHA1-96 for authentication, 3DES-CBC for encryption, 28800 seconds for the lifetime, and group 2 for the PFS group.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 4 destined for Router 1, whereas the

es-return filter matches the return path from Router 1 to Router 4. Apply the **es-traffic** filter to the **so-0/0/0** interface; then apply both the **es-return** filter and the **sa-dynamic** SA to the **es-0/3/0** interface.

Router 3

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.2/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.2;
        destination 10.1.15.1;
      }
      family inet {
        ipsec-sa sa-dynamic; # Apply the dynamic SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.3/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
```

```

        interface so-0/0/0.0;
        interface so-0/0/1.0;
        interface lo0.0;
    }
}
security {
    ipsec {
        proposal es-ipsec-proposal { # Define your IPSec proposal specifications here.
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 28800;
        }
        policy es-ipsec-policy { # Define your IPSec policy specifications here.
            perfect-forward-secrecy {
                keys group2;
            }
            proposals es-ipsec-proposal; # Reference the IPSec proposal here.
        }
        security-association sa-dynamic { # Define your dynamic SA here.
            mode tunnel;
            dynamic {
                ipsec-policy es-ipsec-policy; # Reference the IPSec policy here.
            }
        }
    }
}
ike {
    proposal es-ike-proposal { # Define your IKE proposal specifications here.
        authentication-method pre-shared-keys;
        dh-group group2;
        authentication-algorithm sha1;
        encryption-algorithm 3des-cbc;
        lifetime-seconds 3600;
    }
    policy 10.1.15.1 { # Define your IKE policy specifications here.
        mode main;
        proposals es-ike-proposal; # Reference the IKE proposal here.
        pre-shared-key ascii-text "$ABC123";
        ## The unencrypted preshared key for this example is juniper.
    }
}
firewall {
    filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
        term to-es {
            from {
                source-address {
                    10.1.56.0/24;
                }
                destination-address {
                    10.1.12.0/24;
                }
            }
        }
        then {

```



```

        count ipsec-tunnel;
        ipsec-sa sa-dynamic;
    }
}
term other {
    then accept;
}
}
filter es-return { # Define a filter that matches return IPsec traffic here.
    term return {
        from {
            source-address {
                10.1.12.0/24;
            }
            destination-address {
                10.1.56.0/24;
            }
        }
        then accept;
    }
}
}
}

```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```

[edit]
interfaces {
    so-0/0/0 {
        description "To R3 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.4/32;
            }
        }
    }
}
routing-options {
    router-id 10.0.0.4;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface lo0.0;
        }
    }
}
}

```

Verifying Your Work

To verify proper operation of an IKE-based dynamic SA on the ES PIC, use the following commands:

- **ping**
- **show ike security-associations (detail)**
- **show ipsec security-associations (detail)**
- **traceroute**

The following sections show the output of these commands used with the configuration example:

- [Router 1 on page 118](#)
- [Router 2 on page 119](#)
- [Router 3 on page 120](#)
- [Router 4 on page 121](#)

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface of Router 4 to send traffic across the IPsec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=253 time=0.917 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=253 time=0.881 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=253 time=0.897 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=253 time=0.871 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=253 time=0.890 ms
64 bytes from 10.1.56.2: icmp_seq=5 ttl=253 time=0.858 ms
64 bytes from 10.1.56.2: icmp_seq=6 ttl=253 time=0.904 ms
^C
--- 10.1.56.2 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.858/0.888/0.917/0.019 ms
```

You can also issue the **traceroute** command to verify that traffic to **10.1.56.2** travels over the IPsec tunnel between Router 2 and Router 3. Notice that the second hop does not reference **10.1.15.2**—the physical interface on Router 3. Instead, the loopback address of **10.0.0.3** on Router 3 appears as the second hop. This indicates that the IPSec tunnel is operating correctly.

```
user@R1> traceroute 10.1.56.2
traceroute to 10.1.56.2 (10.1.56.2), 30 hops max, 40 byte packets
 1  10.1.12.1 (10.1.12.1)  0.655 ms  0.549 ms  0.508 ms
 2  10.0.0.3 (10.0.0.3)  0.833 ms  0.786 ms  0.757 ms
```

3 10.1.56.2 (10.1.56.2) 0.808 ms 0.741 ms 0.716 ms

Router 2

Another way to verify that matched traffic is being diverted to the bidirectional IPsec tunnel is to view the firewall filter counter. After you issue the **ping** command from Router 1 (seven packets), the **es-traffic** firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
```

```
Filter: es-traffic
Counters:
Name                               Bytes      Packets
ipsec-tunnel                       588        7
```

After you issue the **ping** command from both Router 1 (seven packets) and Router 4 (five packets), the **es-traffic** firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
```

```
Filter: es-traffic
Counters:
Name                               Bytes      Packets
ipsec-tunnel                       1008       12
```

To verify that the IKE SA negotiation between Routers 2 and 3 is successful, issue the **show ike security-associations detail** command. Notice that the SA contains the settings you specified, such as SHA-1 for the authentication algorithm and 3DES-CBC for the encryption algorithm.

```
user@R2> show ike security-associations detail
```

```
IKE peer 10.1.15.2
Role: Initiator, State: Matured
Initiator cookie: b5dbdfe2f9000000, Responder cookie: a24c868410000041
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 10.1.15.1:500, Remote: 10.1.15.2:500
Lifetime: Expires in 401 seconds
Algorithms:
Authentication      : sha1
Encryption           : 3des-cbc
Pseudo random function: hmac-sha1
Traffic statistics:
Input bytes :          1736
Output bytes :          2652
Input packets:           9
Output packets:          15
Flags: Caller notification sent
IPsec security associations: 3 created, 0 deleted
Phase 2 negotiations in progress: 0
```

To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the SA contains the settings you

specified, such as ESP for the protocol, HMAC-SHA1-96 for the authentication algorithm, and 3DES-CBC for the encryption algorithm.

```
user@R2> show ipsec security-associations detail
```

```
Security association: sa-dynamic, Interface family: Up
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.16.0/24)
Direction: inbound, SPI: 2133029543, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26212 seconds
Hard lifetime: Expires in 26347 seconds
Anti-replay service: Disabled
Direction: outbound, SPI: 1759450863, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26212 seconds
Hard lifetime: Expires in 26347 seconds
Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPsec tunnel. After you issue the **ping** command from Router 1 (seven packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
```

```
Filter: es-traffic
Counters:
Name                               Bytes      Packets
ipsec-tunnel                        588         7
```

After you issue the **ping** command from both Router 1 (seven packets) and Router 4 (five packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
```

```
Filter: es-traffic
Counters:
Name                               Bytes      Packets
ipsec-tunnel                       1008        12
```

To verify the success of the IKE security association, issue the **show ike security-associations detail** command. Notice that the SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ike security-associations detail
```

```
IKE peer 10.1.15.1
Role: Responder, State: Matured
Initiator cookie: b5dbdfe2f9000000, Responder cookie: a24c868410000041
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 10.1.15.2:500, Remote: 10.1.15.1:500
```

```

Lifetime: Expires in 564 seconds
Algorithms:
  Authentication      : sha1
  Encryption          : 3des-cbc
  Pseudo random function: hmac-sha1
Traffic statistics:
  Input bytes  :          2652
  Output bytes :          1856
  Input packets:           15
  Output packets:          10
Flags: Caller notification sent
IPSec security associations: 3 created, 4 deleted
Phase 2 negotiations in progress: 0

```

To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ipsec security-associations detail
```

```

Security association: sa-dynamic, Interface family: Up
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Direction: inbound, SPI: 1759450863, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26427 seconds
Hard lifetime: Expires in 26517 seconds
Anti-replay service: Disabled
Direction: outbound, SPI: 2133029543, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26427 seconds
Hard lifetime: Expires in 26517 seconds
Anti-replay service: Disabled

```

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface of Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
```

```

user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=253 time=13.528 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=253 time=0.873 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=253 time=32.145 ms
64 bytes from 10.1.12.2: icmp_seq=3 ttl=253 time=0.921 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=253 time=0.899 ms
^C
--- 10.1.12.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.873/9.673/32.145/12.255 ms

```

You can also issue the **traceroute** command to verify that traffic to **10.1.12.2** travels over the IPsec tunnel between Router 3 and Router 2. Notice that the second hop does not reference **10.1.15.1**—the physical interface on Router 2. Instead, the loopback address of **10.0.0.2** on Router 2 appears as the second hop. This indicates that the IPsec tunnel is operating correctly.

```
user@R4> traceroute 10.1.12.2
```

```
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
```

```
1  10.1.56.1 (10.1.56.1)  0.681 ms  0.624 ms  0.547 ms
2  10.0.0.2 (10.0.0.2)  0.800 ms  0.770 ms  0.737 ms
3  10.1.12.2 (10.1.12.2)  0.793 ms  0.742 ms  0.716 ms
```

Example: AS PIC IKE Dynamic SA Configuration

Figure 7: AS PIC IKE Dynamic SA Topology Diagram

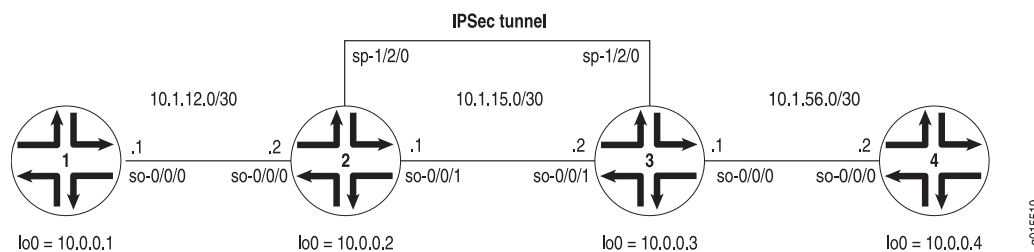


Figure 7 on page 122 shows the same IPsec topology as seen in the AS PIC manual SA example. However, this configuration requires Routers 2 and 3 to establish an IPsec tunnel using an IKE dynamic SA, enhanced authentication, and stronger encryption. Routers 1 and 4 continue to provide basic connectivity and are used to verify that the IPsec tunnel is operational.



NOTE: When you do not specify an IKE proposal, an IPsec proposal, and an IPsec policy on an AS PIC, the Junos OS defaults to the highest level of encryption and authentication. As a result, the default authentication protocol is ESP, the default authentication mode is HMAC-SHA1-96, and the default encryption mode is 3DES-CBC. For more information about default IKE and IPsec policies and proposals on the AS PIC, see [“Configuring IKE Dynamic SAs” on page 66](#).

On Router 1, provide basic OSPF connectivity to Router 2.

Router 1

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
}
```

```

}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.1/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.1;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}
}

```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

Using default values in the AS PIC, you do not need to specify an IPsec proposal, IPsec policy, or IKE proposal. However, you do need to configure a preshared key in an IKE policy with the **pre-shared-key** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. (For more information about default IKE and IPsec policies and proposals on the AS PIC, see [“Configuring IKE Dynamic SAs” on page 66.](#))

To direct traffic into the AS PIC and the IPsec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPsec inside interface into the OSPF configuration.

Router 2

```

[edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.1/30;
      }
    }
  }
}

```

```
}
sp-1/2/0 {
  services-options {
    syslog {
      host local {
        services info;
      }
    }
  }
}
unit 0 {
  family inet {
  }
  unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
    family inet;
    service-domain inside;
  }
  unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
    family inet;
    service-domain outside;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.2/32;
    }
  }
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
      interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
    }
  }
}
services {
  service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
    next-hop-service { # Required for dynamic routing protocols such as OSPF.
      inside-service-interface sp-1/2/0.1;
      outside-service-interface sp-1/2/0.2;
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.1; # Specify the local IP address of the IPSec tunnel.
    }
    ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
  }
  ipsec-vpn {
    rule rule-ike { # Define your IPSec VPN rule here.
      term term-ike {
```



```

    then {
        remote-gateway 10.1.15.2; # The remote IP address of the IPSec tunnel.
        dynamic { # This creates a dynamic SA.
            ike-policy ike-policy-preshared; # Reference your IKE policy here.
        }
    }
}
match-direction input; # Specify in which direction the rule should match.
}
ike {
    policy ike-policy-preshared { # Define your IKE policy specifications here.
        pre-shared-key ascii-text "$ABC123";
        ## The unencrypted preshared key for this example is juniper.
    }
}
}
}
}
}

```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

Again, use the same default policies and proposals that you used on Router 2. However, remember to configure a preshared key in an IKE policy with the **pre-shared-key** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. The key must match the one you specified on Router 2. (For more information about default IKE and IPSec policies and proposals on the AS PIC, see [“Configuring IKE Dynamic SAs” on page 66.](#))

To direct traffic into the AS PIC and the IPSec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPSec inside interface into the OSPF configuration.

Router 3

```

[edit]
interfaces {
    so-0/0/0 {
        description "To R4 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.1/30;
            }
        }
    }
    so-0/0/1 {
        description "To R2 so-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.2/30;
            }
        }
    }
    sp-1/2/0 {

```

```
services-options {
  syslog {
    host local {
      services info;
    }
  }
}
unit 0 {
  family inet {
  }
  unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
    family inet;
    service-domain inside;
  }
  unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
    family inet;
    service-domain outside;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.3/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
      interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
    }
  }
}
}
services {
  service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
    next-hop-service { # Required for dynamic routing protocols such as OSPF.
      inside-service-interface sp-1/2/0.1;
      outside-service-interface sp-1/2/0.2;
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.2; # Specify the local IP address of the IPSec tunnel.
    }
    ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
  }
  ipsec-vpn {
    rule rule-ike { # Define your IPSec VPN rule here.
      term term-ike {
        then {
          remote-gateway 10.1.15.1; # The remote IP address of the IPSec tunnel.
        }
      }
    }
  }
}
```

```

        dynamic { # This creates a dynamic SA.
            ike-policy ike-policy-preshared; # Reference your IKE policy here.
        }
    }
    match-direction input; # Specify in which direction the rule should match.
}
ike {
    policy ike-policy-preshared { # Define your IKE policy specifications here.
        pre-shared-key ascii-text "$ABC123";
        ## The unencrypted preshared key for this example is juniper.
    }
}
}
}
}

```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```

[edit]
interfaces {
    so-0/0/0 {
        description "To R3 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.4/32;
            }
        }
    }
}
routing-options {
    router-id 10.0.0.4;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface lo0.0;
        }
    }
}
}

```

Verifying Your Work

To verify proper operation of an IKE-based dynamic SA on the AS PIC, use the following commands:

- **ping**
- **show services ipsec-vpn ike security-associations (detail)**
- **show services ipsec-vpn ipsec security-associations (detail)**
- **show services ipsec-vpn ipsec statistics**
- **traceroute**

The following sections show the output of these commands used with the configuration example:

- [Router 1 on page 128](#)
- [Router 2 on page 128](#)
- [Router 3 on page 129](#)
- [Router 4 on page 130](#)

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface on Router 4 to send traffic across the IPSec tunnel.

```
user@R1> ping 10.1.56.2

PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=254 time=1.351 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=254 time=1.187 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=254 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=254 time=1.154 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=254 time=1.156 ms
^C
--- 10.1.56.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.154/1.204/1.351/0.074 ms
```

Router 2

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations** command.

```
user@R2> show services ipsec-vpn ike security-associations
```

Remote Address	State	Initiator cookie	Responder cookie	Exchange type
10.1.15.2	Matured	03075bd3a0000003	4bff26a5c7000003	Main

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the default

settings inherent in the AS PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: service-set-dynamic-BiEspsha3des
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.16.0/24)
Direction: inbound, SPI: 2666326758, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26863 seconds
Hard lifetime: Expires in 26998 seconds
Anti-replay service: Enabled, Replay window size: 64
Direction: outbound, SPI: 684772754, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26863 seconds
Hard lifetime: Expires in 26998 seconds
Anti-replay service: Enabled, Replay window size: 64
```

To verify that traffic is traveling over the bidirectional IPSec tunnel, issue the **show services ipsec-vpn statistics** command:

```
user@R2> show services ipsec-vpn ipsec statistics
```

```
PIC: sp-1/2/0, Service set: service-set-dynamic-BiEspsha3des
ESP Statistics:
  Encrypted bytes:      2248
  Decrypted bytes:      2120
  Encrypted packets:    27
  Decrypted packets:    25
AH Statistics:
  Input bytes:          0
  Output bytes:         0
  Input packets:        0
  Output packets:       0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
```

Bad headers: 0, Bad trailers: 0

Router 3

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ike security-associations
```

Remote Address	State	Initiator cookie	Responder cookie	Exchange type
10.1.15.1	Matured	03075bd3a0000003	4bff26a5c7000003	Main

To verify that the IPsec SA is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: service-set-dynamic-BiEspsha3des
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Direction: inbound, SPI: 684772754, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26598 seconds
Hard lifetime: Expires in 26688 seconds
Anti-replay service: Enabled, Replay window size: 64
Direction: outbound, SPI: 2666326758, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26598 seconds
Hard lifetime: Expires in 26688 seconds
Anti-replay service: Enabled, Replay window size: 64
```

To verify that traffic is traveling over the bidirectional IPsec tunnel, issue the **show services ipsec-vpn statistics** command:

```
user@R3> show services ipsec-vpn ipsec statistics
```

```
PIC: sp-1/2/0, Service set: service-set-dynamic-BiEspsha3des
ESP Statistics:
  Encrypted bytes:      2120
  Decrypted bytes:      2248
  Encrypted packets:    25
  Decrypted packets:    27
AH Statistics:
  Input bytes:          0
  Output bytes:         0
  Input packets:        0
  Output packets:       0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
```

Bad headers: 0, Bad trailers: 0

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface on Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
```

```
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
```

```

64 bytes from 10.1.12.2: icmp_seq=3 ttl=254 time=1.142 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=254 time=1.139 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms

```

The final way you can confirm that traffic travels over the IPsec tunnel is by issuing the **tracert** command to the **so-0/0/0** interface on Router 1. Notice that the physical interface between Routers 2 and 3 is not referenced in the path; traffic enters the IPsec tunnel through the adaptive services IPsec inside interface on Router 3, passes through the loopback interface on Router 2, and ends at the **so-0/0/0** interface on Router 1.

```

user@R4> traceroute 10.1.12.2

traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1  10.1.15.2 (10.1.15.2)  0.987 ms  0.630 ms  0.563 ms
 2  10.0.0.2 (10.0.0.2)    1.194 ms  1.058 ms  1.033 ms
 3  10.1.12.2 (10.1.12.2)  1.073 ms  0.949 ms  0.932 ms

```

Example: IKE Dynamic SA Between an AS PIC and an ES PIC Configuration

Figure 8: AS PIC to ES PIC IKE Dynamic SA Topology Diagram

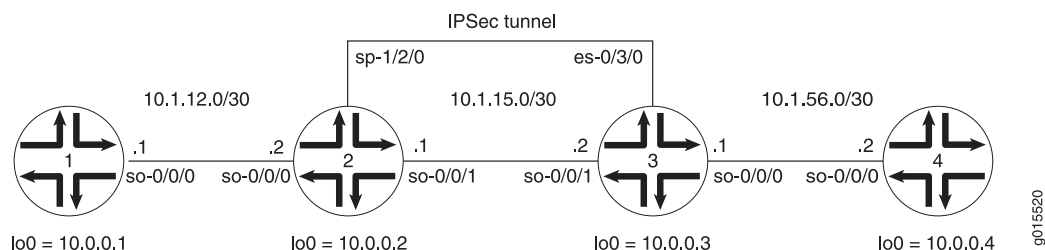


Figure 8 on page 131 shows a hybrid configuration that allows you to create an IPsec tunnel between the AS PIC and the ES PIC. Router 2 contains an AS PIC at **sp-1/2/0** and Router 3 has an ES PIC at **es-0/3/0**. To establish an IPsec tunnel using an IKE dynamic SA, the key is to learn the default IKE SA and IPsec SA settings built into the AS PIC and configure them explicitly on the ES PIC. Routers 1 and 4 again provide basic connectivity and are used to verify that the IPsec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

```

Router 1 [edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
}

```

```

}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.1/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.1;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}
}

```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

Using default values in the AS PIC, you do not need to specify an IPsec proposal, IPsec policy, or IKE proposal. However, you do need to configure a preshared key in an IKE policy with the **pre-shared-key** statement at the **[edit services ipsec-vpn ike policy policy-name]** hierarchy level. (For more information about default IKE and IPsec policies and proposals on the AS PIC, see [“Configuring IKE Dynamic SAs” on page 66.](#))

To direct traffic into the AS PIC and the IPsec tunnel, include match conditions in the **rule-ike** IPsec VPN rule to match inbound traffic from Router 1 that is destined for Router 4. Because the rule is already referenced by the service set, apply the service set to the **so-0/0/1** interface. To count the amount of traffic that enters the IPsec tunnel, configure a firewall filter called **ipsec-tunnel** and apply it to the **sp-1/2/0** interface.

Router 2

```

[edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {

```



```

service { # Apply the service set here.
  input {
    service-set service-set-dynamic-BiEspsha3des;
  }
  output {
    service-set service-set-dynamic-BiEspsha3des;
  }
}
address 10.1.15.1/30;
}
}
sp-1/2/0 {
  services-options {
    syslog {
      host local {
        services info;
      }
    }
  }
  unit 0 {
    family inet {
      filter {
        input ipsec-tunnel; # Apply the firewall filter with the counter here.
      }
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.2/32;
    }
  }
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
firewall {
  filter ipsec-tunnel { # Configure a firewall filter to count IPsec traffic here.
    term 1 {
      then {
        count ipsec-tunnel;
        accept;
      }
    }
  }
}

```

```

    }
  }
}
services {
  service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
    interface-service {
      service-interface sp-1/2/0; # Specify an interface to process IPsec.
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.1; # Specify the local IP address of the IPsec tunnel.
    }
    ipsec-vpn-rules rule-ike; # Reference your IPsec VPN rule here.
  }
  ipsec-vpn {
    rule rule-ike { # Define your IPsec VPN rule here.
      term term-ike {
        from {
          source-address {
            10.1.12.0/24;
          }
          destination-address {
            10.1.56.0/24;
          }
        }
        then {
          remote-gateway 10.1.15.2; # The remote IP address of the IPsec tunnel.
          dynamic { # This creates a dynamic SA.
            ike-policy ike-policy-preshared; # Reference your IKE proposal here.
          }
        }
      }
      match-direction output; # Specify in which direction the rule should match.
    }
    ike {
      policy ike-policy-preshared { # Define your IKE policy specifications here.
        pre-shared-key ascii-text "$ABC123";
        ## The unencrypted preshared key for this example is juniper.
      }
    }
  }
}
}

```

Router 2

```

[edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.1/30;
      }
    }
  }
}

```

```
so-0/0/1 {
  description "To R3 so-0/0/1";
  unit 0 {
    family inet {
      service { # Apply the service set here.
        input {
          service-set service-set-dynamic-BiEspsha3des;
        }
        output {
          service-set service-set-dynamic-BiEspsha3des;
        }
      }
      address 10.1.15.1/30;
    }
  }
}
sp-1/2/0 {
  services-options {
    syslog {
      host local {
        services info;
      }
    }
  }
  unit 0 {
    family inet {
      filter {
        input ipsec-tunnel; # Apply the firewall filter with the counter here.
      }
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.2/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
}
firewall {
  filter ipsec-tunnel { # Configure a firewall filter to count IPSec traffic here.
```

```

    term 1 {
        then {
            count ipsec-tunnel;
            accept;
        }
    }
}
}
services {
    service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
        interface-service {
            service-interface sp-1/2/0; # Specify an interface to process IPSec.
        }
        ipsec-vpn-options {
            local-gateway 10.1.15.1; # Specify the local IP address of the IPSec tunnel.
        }
        ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
    }
    ipsec-vpn {
        rule rule-ike { # Define your IPSec VPN rule here.
            term term-ike {
                from {
                    source-address {
                        10.1.12.0/24;
                    }
                    destination-address {
                        10.1.56.0/24;
                    }
                }
                then {
                    remote-gateway 10.1.15.2; # The remote IP address of the IPSec tunnel.
                    dynamic { # This creates a dynamic SA.
                        ike-policy ike-policy-preshared; # Reference your IKE proposal here.
                    }
                }
            }
            match-direction output; # Specify in which direction the rule should match.
        }
        ike {
            policy ike-policy-preshared { # Define your IKE policy specifications here.
                pre-shared-key ascii-text "$ABC123";
                ## The unencrypted preshared key for this example is juniper.
            }
        }
    }
}
}

```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA called **sa-dynamic** at the **[edit security ipsec security-association]** hierarchy level. To allow the ES PIC to communicate with the IKE dynamic SA established on Router 2, you must explicitly configure the same policies and proposals on the ES PIC that are available by default on the AS PIC. (For more information about default IKE and IPSec policies and proposals on the AS PIC, see [“Configuring IKE Dynamic SAs” on page 66.](#))

For your IKE policy and proposal, use preshared keys for the authentication method, SHA-1 for the authentication algorithm, 3DES-CBC for encryption, group 2 for the Diffie-Hellman group, main mode, 3600 seconds for the lifetime, and a preshared key of **juniper** for the initial IKE negotiation. For your IPSec policy and proposal, use ESP for the protocol, HMAC-SHA1-96 for authentication, 3DES-CBC for encryption, 28800 seconds for the lifetime, and group 2 for the PFS group.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 4 destined for Router 1, whereas the **es-return** filter matches the return path from Router 1 to Router 4. Apply the **es-traffic** filter to the **so-0/0/0** interface; then apply both the **es-return** filter and the **sa-dynamic SA** to the **es-0/3/0** interface.

Router 3

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.2/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.2;
        destination 10.1.15.1;
      }
      family inet {
        ipsec-sa sa-dynamic; # Apply the dynamic SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.3/32;
      }
    }
  }
}
```

```

    }
  }
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
security {
  ipsec {
    proposal es-ipsec-proposal { # Define your IPSec proposal specifications here.
      protocol esp;
      authentication-algorithm hmac-sha1-96;
      encryption-algorithm 3des-cbc;
      lifetime-seconds 28800;
    }
    policy es-ipsec-policy { # Define your IPSec policy specifications here.
      perfect-forward-secrecy {
        keys group2;
      }
      proposals es-ipsec-proposal; # Reference the IPSec proposal here.
    }
    security-association sa-dynamic { # Define your dynamic SA here.
      mode tunnel;
      dynamic {
        ipsec-policy es-ipsec-policy; # Reference the IPSec policy here.
      }
    }
  }
}
ike {
  proposal es-ike-proposal { # Define your IKE proposal specifications here.
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 3600;
  }
  policy 10.1.15.1 { # Define your IKE policy specifications here.
    mode main;
    proposals es-ike-proposal; # Reference the IKE proposal here.
    pre-shared-key ascii-text "$ABC123";
    ## The unencrypted preshared key for this example is juniper.
  }
}
}

```

```

firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-dynamic;
      }
    }
    term other {
      then accept;
    }
  }
  filter es-return { # Define a filter that matches return IPSec traffic here.
    term return {
      from {
        source-address {
          10.1.12.0/24;
        }
        destination-address {
          10.1.56.0/24;
        }
      }
      then accept;
    }
  }
}

```

Router 4

```

[edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}

```

```
    }  
  }  
  routing-options {  
    router-id 10.0.0.4;  
  }  
  protocols {  
    ospf {  
      area 0.0.0.0 {  
        interface so-0/0/0.0;  
        interface lo0.0;  
      }  
    }  
  }  
}
```

Verifying Your Work

To verify proper operation of an IKE-based dynamic SA on the AS PIC, use the following commands:

- **ping**
- **show services ipsec-vpn ike security-associations (detail)**
- **show services ipsec-vpn ipsec security-associations (detail)**
- **traceroute**

To verify proper operation of an IKE-based dynamic SA on the ES PIC, use the following commands:

- **ping**
- **show ike security-associations (detail)**
- **show ipsec security-associations (detail)**
- **traceroute**

The following sections show the output of these commands used with the configuration example:

- [Router 1 on page 140](#)
- [Router 2 on page 141](#)
- [Router 3 on page 143](#)
- [Router 4 on page 144](#)

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface of Router 4 to send traffic across the IPSec tunnel.

```
user@R1> ping 10.1.56.2
```



```

PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=253 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=253 time=1.020 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=253 time=0.998 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=253 time=1.037 ms
^C
--- 10.1.56.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.998/1.057/1.172/0.068 ms

```

You can also issue the **tracert** command to verify that traffic to **10.1.56.2** travels over the IPsec tunnel between Router 2 and Router 3. Notice that the traced path does not reference **10.1.15.2**—the physical interface on Router 3. Instead, traffic arriving at Router 2 is immediately filtered into the IPsec tunnel and the path is listed as unknown with the ******* notation. This indicates that the IPsec tunnel is operating correctly.

```

user@R1> tracert 10.1.56.2

tracert to 10.1.56.2 (10.1.56.2), 30 hops max, 40 byte packets
 1 * * *
 2 10.1.56.2 (10.1.56.2) 1.045 ms 0.915 ms 0.850 ms

```

Router 2

One way to verify that matched traffic is being diverted to the bidirectional IPsec tunnel is to view the firewall filter counter. Before any traffic flows, the **ipsec-tunnel** firewall filter counter looks like this:

```

user@R2> show firewall filter ipsec-tunnel

Filter: ipsec-tunnel
Counters:

```

Name	Bytes	Packets
ipsec-tunnel	0	0

After you issue the **ping** command from Router 1 (four packets) to **10.1.56.2**, the **ipsec-tunnel** firewall filter counter looks like this:

```

user@R2> show firewall filter ipsec-tunnel

Filter: ipsec-tunnel
Counters:

```

Name	Bytes	Packets
ipsec-tunnel	336	4

After you issue the **ping** command from both Router 1 to **10.1.56.2** (four packets) and from Router 4 to **10.1.12.2** (six packets), the **ipsec-tunnel** firewall filter counter looks like this:

```

user@R2> show firewall filter ipsec-tunnel

Filter: es-traffic
Counters:

```

Name	Bytes	Packets
ipsec-tunnel	840	10

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations detail** command. Notice that the SA contains the default IKE settings inherent in the AS PIC, such as SHA-1 for the authentication algorithm and 3DES-CBC for the encryption algorithm.

```
user@R2> show services ipsec-vpn ike security-associations detail
```

```
IKE peer 10.1.15.2
  Role: Responder, State: Matured
  Initiator cookie: c8e1e4c0da000040, Responder cookie: 4fbaa5184e000044
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.15.1:500, Remote: 10.1.15.2:500
  Lifetime: Expires in 3535 seconds
  Algorithms:
    Authentication      : sha1
    Encryption          : 3des-cbc
    Pseudo random function: hmac-sha1
  Traffic statistics:
    Input bytes      :      840
    Output bytes     :      756
    Input packets    :         5
    Output packets   :         4
  Flags: Caller notification sent
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0
```

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the default settings inherent in the AS PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: service-set-dynamic-BiEspsha3des
  Rule: rule-ike, Term: term-ike, Tunnel index: 1
  Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
  Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
  Remote identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
  Direction: inbound, SPI: 407204513, AUX-SPI: 0
  Mode: tunnel, Type: dynamic, State: Installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
  Soft lifetime: Expires in 24546 seconds
  Hard lifetime: Expires in 24636 seconds
  Anti-replay service: Disabled
  Direction: outbound, SPI: 2957235894, AUX-SPI: 0
  Mode: tunnel, Type: dynamic, State: Installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
  Soft lifetime: Expires in 24546 seconds
  Hard lifetime: Expires in 24636 seconds
  Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPsec tunnel. After you issue the **ping** command from Router 1 (four packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
```

```
Filter: es-traffic
Counters:
Name                               Bytes      Packets
ipsec-tunnel                       336         4
```

After you issue the **ping** command from both Router 1 (four packets) and Router 4 (six packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
```

```
Filter: es-traffic
Counters:
Name                               Bytes      Packets
ipsec-tunnel                       840        10
```

To verify the success of the IKE security association on the ES PIC, issue the **show ike security-associations detail** command. Notice that the IKE SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ike security-associations detail
```

```
IKE peer 10.1.15.1
Role: Initiator, State: Matured
Initiator cookie: c8e1e4c0da000040, Responder cookie: 4fbaa5184e000044
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 10.1.15.2:500, Remote: 10.1.15.1:500
Lifetime: Expires in 3441 seconds
Algorithms:
Authentication      : sha1
Encryption           : 3des-cbc
Pseudo random function: hmac-sha1
Traffic statistics:
Input bytes  :          756
Output bytes :          840
Input packets:           4
Output packets:         5
Flags: Caller notification sent
IPSec security associations: 1 created, 0 deleted
Phase 2 negotiations in progress: 0
```

To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the IPsec SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ipsec security-associations detail
```

```

Security association: sa-dynamic, Interface family: Up
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Direction: inbound, SPI: 2957235894, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 28555 seconds
Hard lifetime: Expires in 28690 seconds
Anti-replay service: Disabled
Direction: outbound, SPI: 407204513, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 28555 seconds
Hard lifetime: Expires in 28690 seconds
Anti-replay service: Disabled

```

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface on Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
```

```

PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
64 bytes from 10.1.12.2: icmp_seq=3 ttl=254 time=1.142 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=254 time=1.139 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms

```

Again, the **traceroute** command verifies that traffic to **10.1.12.2** travels over the IPsec tunnel between Router 3 and Router 2. Notice that the second hop does not reference **10.1.15.1**—the physical interface on Router 2. Instead, the second hop is listed as unknown with the ******* notation. This indicates that the IPsec tunnel is operating correctly.

```
user@R4> traceroute 10.1.12.2
```

```

traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1  10.1.56.1 (10.1.56.1)  3.561 ms  0.613 ms  0.558 ms
 2  * * *
 3  10.1.12.2 (10.1.12.2)  1.073 ms  0.862 ms  0.818 ms

```

Example: AS PIC IKE Dynamic SA with Digital Certificates Configuration

Figure 9: AS PIC IKE Dynamic SA Topology Diagram

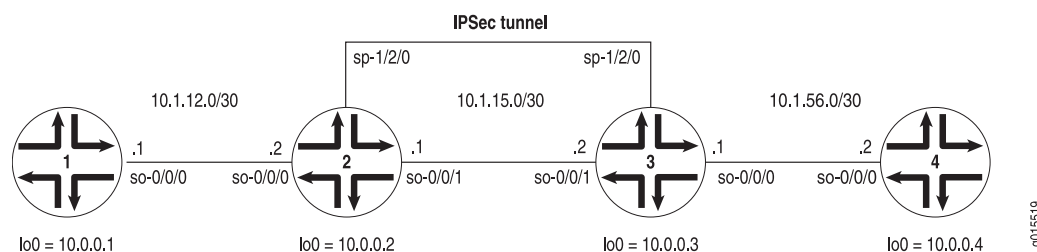


Figure 9 on page 145 shows the same IPSec topology as the AS PIC dynamic SA example on “Example: AS PIC IKE Dynamic SA Configuration” on page 122. However, this configuration requires Routers 2 and 3 to establish an IKE-based IPSec tunnel by using digital certificates in place of preshared keys. Routers 1 and 4 continue to provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

```
Router 1 [edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.1/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.1;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}
```

On Router 2, you must request a CA certificate, create a local certificate, and load these digital certificates into the router before you can reference them in your IPSec

configuration. To begin, configure an IPSec profile by specifying the trusted CA and URL of the CA server that handles CA certificate processing:

```
[edit]
security {
  pki {
    ca-profile entrust {
      ca-identity entrust;
      enrollment {
        url http://ca-1.example.com/cgi-bin/pkiclient.exe;
      }
    }
  }
}
```

Certificate revocation list (CRL) verification is enabled by default. You can optionally specify the Lightweight Access Directory (LDAP) server where the CA stores the CRL. The certificate typically includes a certificate distribution point (CDP), which contains information about how to retrieve the CRL for the certificate. The router uses this information to download the CRL automatically. In this example, the LDAP URL is specified, which overrides the location provided in the certificate:

```
[edit]
security pki ca-profile entrust {
  revocation-check {
    crl {
      url ldap://10.157.90.185/o=juniper,c=uscertificateRevocationListbase;
    }
  }
}
```

After you configure the CA profile, you can request a CA certificate from the trusted CA. In this example, the certificate is enrolled online and installed into the router automatically.

```
user@R2> request security pki ca-certificate enroll ca-profile entrust
```

Received following certificates:

```
Certificate: C=us, O=juniper
Fingerprint: 00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
Certificate: C=us, O=juniper, CN=First Officer
Fingerprint: bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
Certificate: C=us, O=juniper, CN=First Officer
Fingerprint: 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
Do you want to load the above CA certificate ? [yes,no] (no) yes
```



NOTE: If you obtain the CA certificate directly from the CA (for example, as an e-mail attachment or website download), you can install it with the `request security pki ca-certificate load` command.

Next, you must generate a private/public key pair before you can create a local certificate.

```
user@R2> request security pki generate-key-pair certificate-id local-entrust2
```

```
Generated key pair local-entrust2, key size 1024 bits
```

When the key pair is available, generate a local certificate request and send it to the CA for processing.

```
user@R2> request security pki generate-certificate-request
```

```
certificate-id local-entrust2 domain-name router2.example.com
```

```
filename entrust-req2 subject cn=router2.example.com
```

```
Generated certificate request
```

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHAXLmp1bm1wZXIubmVOMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFk1Qws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8E1wTJ1kmIt2cB3yi fB6zePd+6WYpf57Crwre7YqPkIXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8o0Xyqog8ACDFVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjA0BGNVHQ8BAF8EBAMCB4AwJAYD
VR0RAQH/BBowGIIwDHAXLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBC2rq1v5SOQXH7LCb/FdqAL8ZM6GoaNs5d6cGwq4bB6a7UQFgtH406gQ3G
3iH0Zfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteo1ZCiZ70f09Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
```

```
-----END CERTIFICATE REQUEST-----
```

```
Fingerprint:
```

```
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
```

```
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```



NOTE: You can request the creation and installation of a local certificate online with the `request security pki local-certificate enroll` command. For more information, see [“Generating and Enrolling a Local Digital Certificate” on page 76](#) or the *Junos System Basics and Services Command Reference*.

The trusted CA digitally signs the local certificate and returns it to you. Copy the certificate file into the router and load the certificate.

```
user@R2> request security pki local-certificate load filename /tmp/router2-cert certificate-id local-entrust2
```

```
Local certificate local-entrust2 loaded successfully
```



NOTE: The name of the file sent to you by the CA might not match the name of the certificate identifier. However, the certificate-id name must always match the name of the key pair you generated for the router.

After the local and CA certificates have been loaded, you can reference them in your IPsec configuration.

Using default values in the AS PIC, you do not need to configure an IPsec proposal or IPsec policy. However, you must configure an IKE proposal that specifies the use of digital certificates, reference the IKE proposal and local certificate in an IKE policy, and apply the CA profile to the service set. To enable an IKE proposal for digital certificates, include the **rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal *proposal-name* authentication-method]** hierarchy level. To reference the local certificate in the IKE policy, include the **local-certificate** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. To identify the CA or RA in the service set, include the **trusted-ca** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.



NOTE: For more information about default IKE and IPsec policies and proposals on the AS PIC, see [“Configuring IKE Dynamic SAs” on page 66](#).

Optionally, you can configure automatic reenrollment of the certificate with the **auto-re-enrollment** statement at the **[edit security pki]** hierarchy level.

The remaining configuration components of your IKE-based IPsec tunnel are the same as when you use preshared keys. Enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

To direct traffic into the AS PIC and the IPsec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPsec inside interface into the OSPF configuration.

Router 2

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.1/30;
      }
    }
  }
  sp-1/2/0 {
    unit 0 {
      family inet;
    }
  }
}
```



```

    }
    unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
        family inet;
        service-domain inside;
    }
    unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
        family inet;
        service-domain outside;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.0.0.2/32;
        }
    }
}
}
routing-options {
    router-id 10.0.0.2;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
            interface lo0.0;
        }
    }
}
}
security { # Configure CA profiles here, including the URLs used to reach the CAs.
    pki {
        ca-profile entrust {
            ca-identity entrust;
            enrollment {
                url http://ca-1.example.com/cgi-bin/pkiclient.exe;
            }
            revocation-check {
                crl {
                    url ldap://10.157.90.185/o=juniper,c=uscertificateRevocationListbase;
                    # Specify the URL of the LDAP server where the CA stores the CRL.
                }
            }
        }
        ca-profile microsoft {
            ca-identity microsoft;
            enrollment {
                url http://192.168.11.78:80/certsrv/mscep/mscep.dll;
            }
        }
        ca-profile verisign {
            ca-identity verisign;
            enrollment {
                url http://pilotonsiteipsec.verisign.com/cgi-bin/pkiclient.exe;
            }
        }
    }
}

```

```

    }
  }
}
services {
  service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
    next-hop-service { # Required for dynamic routing protocols such as OSPF.
      inside-service-interface sp-1/2/0.1;
      outside-service-interface sp-1/2/0.2;
    }
    ipsec-vpn-options {
      trusted-ca entrust; # Reference the CA profile here.
      local-gateway 10.1.15.1; # Specify the local IP address of the IPsec tunnel.
    }
    ipsec-vpn-rules rule-ike; # Reference your IPsec VPN rule here.
  }
  ipsec-vpn {
    rule rule-ike { # Define your IPsec VPN rule here.
      term term-ike {
        then {
          remote-gateway 10.1.15.2; # The remote IP address of the IPsec tunnel.
          dynamic { # This creates a dynamic SA.
            ike-policy ike-digital-certificates; # Reference your IKE policy here.
          }
        }
      }
      match-direction input; # Specify in which direction the rule should match.
    }
    ike {
      proposal ike-proposal {
        authentication-method rsa-signatures; # Uses digital certificates
      }
      policy ike-digital-certificates {
        proposals ike-proposal; # Apply the IKE proposal here.
        local-id fqdn router2.example.com; # Provide an identifier for the local router.
        local-certificate local-entrust2; # Reference the local certificate here.
        remote-id fqdn router3.example.com; # Provide an ID for the remote router.
      }
    }
    establish-tunnels immediately;
  }
}

```

On Router 3, you must repeat the digital certificate procedures you performed on Router 2. If the IPsec peers do not have a symmetrical configuration containing all the necessary components, they cannot establish a peering relationship.

You need to request a CA certificate, create a local certificate, load these digital certificates into the router, and reference them in your IPsec configuration. Begin by configuring an IPsec CA profile. Include the **ca-profile** statement at the **[edit security pki]** hierarchy level and specify the trusted CA and URL of the CA server that handles CA certificate processing. Include the CRL statements found on Router 2 to complete your CA profile on Router 3.

After you configure the CA profile, request a CA certificate from the trusted CA. In this example, the certificate is enrolled online and installed into the router automatically.

```
user@R3> request security pki ca-certificate enroll ca-profile entrust
```

Received following certificates:

```
Certificate: C=us, O=juniper
  Fingerprint: 00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
Certificate: C=us, O=juniper, CN=First Officer
  Fingerprint: bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
Certificate: C=us, O=juniper, CN=First Officer
  Fingerprint: 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
Do you want to load the above CA certificate ? [yes,no] (no) yes
```



NOTE: If you obtain the CA certificate directly from the CA (for example, as an e-mail attachment or website download), you can install it with the `request security pki ca-certificate load` command.

Next, generate a private/public key pair.

```
user@R3> request security pki generate-key-pair certificate-id local-entrust3
```

Generated key pair local-entrust3, key size 1024 bits

When the key pair is available, you can generate a local certificate request and send it to the CA for processing.

```
user@R3> request security pki generate-certificate-request
```

```
certificate-id local-entrust3 domain-name router3.example.com
filename entrust-req3 subject cn=router3.example.com
Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIB8jCCAVsCAQAwZTEYMBYGA1UEAxMPdHA1Lmp1bm1wZXIubmVOMRQwEgYDVQQL
EwtFbmdpbmVlcm1uZzEQMA4GA1UEChMHbnVuaXB1cjETMBEGA1UECBMKQ2FsaWZv
cm5pYTEMMAoGA1UEBhMDVVBmIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCg
Wjo50w8jrnphs0sRFvqQMwC6P1Ya65thrJ8nHZ2qgYgRbSr08hd0DhvU6/5VuD2/
zBtgV5ZSA01yV6DXq1bVj/2XirQAJMRCr1eYu6DhYRBMNq/UaQv4Z8Sse1EJv+uR
HTNbD7x1wpw2zwz1tRuGFtFr/FrGB0hF7IE+Xm5e2wIDAQABoE0wSwYJKoZIhvcN
AQkOMT4wPDA0BgNVHQ8BAf8EBAMCB4AwKgYDVR0RAQH/BCAwHocEwKhGk4IwDHA1
LmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQFAAOBgQBbiJ+ZCeQ59/eY
4Rd6awIpJFTz0svRZLxxjFWogusVTmaD2dsqFBqftS1eJBdeiuRcYMF9vOn0GKm
FNfouegwei5+vzdNmNo55eIb3rs4pP62q0W5CUgmbHrjtp31yJsvu0xTTcPNY8zw
b6GyM2Hdkk3Vh2ReX11tQUSqYujTjw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
7c:e8:f9:45:93:8d:a3:92:7f:18:29:02:f1:c8:e2:85:3d:ad:df:1f (sha1)
00:4e:df:a0:6b:ad:8c:50:da:7c:a1:cf:5d:37:b0:ea (md5)
```

The trusted CA digitally signs the local certificate and returns it to you. Copy the certificate file into the router and load the certificate.

```
user@R3> request security pki local-certificate load filename /tmp/router3-cert certificate-id
local-entrust3
```

```
Local certificate local-entrust3 loaded successfully
```

After the local and CA certificates have been loaded, you can reference them in your IPsec configuration. Using default values in the AS PIC, you do not need to configure an IPsec proposal or IPsec policy. However, you must configure an IKE proposal that uses digital certificates, reference the IKE proposal and local certificate in an IKE policy, and apply the CA profile to the service set. To enable the IKE proposal for digital certificates, include the **rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal proposal-name authentication-method]** hierarchy level. To reference the local certificate in the IKE policy, include the **local-certificate** statement at the **[edit services ipsec-vpn ike policy policy-name]** hierarchy level. To identify the CA or RA in the service set, include the **trusted-ca** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level.

The remaining configuration components of your IKE-based IPsec tunnel are the same as when you use preshared keys. Enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

To direct traffic into the AS PIC and the IPsec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPsec inside interface into the OSPF configuration.

Router 3

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.2/30;
      }
    }
  }
  sp-1/2/0 {
    unit 0 {
      family inet;
    }
    unit 1 { # sp-1/2/0.1 is the IPsec inside interface.
      family inet;
      service-domain inside;
    }
    unit 2 { # sp-1/2/0.2 is the IPsec outside interface.
```

```

        family inet;
        service-domain outside;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.0.0.3/32;
        }
    }
}
routing-options {
    router-id 10.0.0.3;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
            interface lo0.0;
        }
    }
}
security { # Configure CA profiles here, including the URLs used to reach the CAs.
    pki {
        ca-profile entrust {
            ca-identity entrust;
            enrollment {
                url http://ca-1.example.com/cgi-bin/pkiclient.exe;
            }
            revocation-check {
                crl {
                    url ldap://10.157.90.185/o=juniper,c=uscertificateRevocationListbase;
                    # Specify the URL of the LDAP server where the CA stores the CRL.
                }
            }
        }
        ca-profile microsoft {
            ca-identity microsoft;
            enrollment {
                url http://192.168.11.78:80/certsrv/mscep/mscep.dll;
            }
        }
        ca-profile verisign {
            ca-identity verisign;
            enrollment {
                url http://pilotonsiteipsec.verisign.com/cgi-bin/pkiclient.exe;
            }
        }
    }
}
services {
    service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
        next-hop-service { # Required for dynamic routing protocols such as OSPF.

```

```

inside-service-interface sp-1/2/0.1;
outside-service-interface sp-1/2/0.2;
}
ipsec-vpn-options {
    trusted-ca entrust; # Reference the CA profile here.
    local-gateway 10.1.15.2; # Specify the local IP address of the IPsec tunnel.
}
ipsec-vpn-rules rule-ike; # Reference your IPsec VPN rule here.
}
ipsec-vpn {
    rule rule-ike { # Define your IPsec VPN rule here.
        term term-ike {
            then {
                remote-gateway 10.1.15.1; # The remote IP address of the IPsec tunnel.
                dynamic { # This creates a dynamic SA.
                    ike-policy ike-digital-certificates; # Reference your IKE policy here.
                }
            }
        }
        match-direction input; # Specify in which direction the rule should match.
    }
    ike {
        proposal ike-proposal {
            authentication-method rsa-signatures; # Uses digital certificates
        }
        policy ike-digital-certificates {
            proposals ike-proposal; # Apply the IKE proposal here.
            local-id fqdn router3.example.com; # Provide an identifier for the local router.
            local-certificate local-entrust3; # Reference the local certificate here.
            remote-id fqdn router2.example.com; # Provide an ID for the remote router.
        }
    }
    establish-tunnels immediately;
}
}

```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```

[edit]
interfaces {
    so-0/0/0 {
        description "To R3 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.4/32;
            }
        }
    }
}

```

```

    }
  }
  routing-options {
    router-id 10.0.0.4;
  }
  protocols {
    ospf {
      area 0.0.0.0 {
        interface so-0/0/0.0;
        interface lo0.0;
      }
    }
  }
}

```

Verifying Your Work

To verify proper operation of an IKE-based dynamic SA on the AS PIC, use the following commands:

- **ping**
- **show services ipsec-vpn certificates (detail)**
- **show services ipsec-vpn ike security-associations (detail)**
- **show services ipsec-vpn ipsec security-associations (detail)**
- **show services ipsec-vpn ipsec statistics**
- **traceroute**

To verify and manage digital certificates in your router, use the following commands:

- **show security pki ca-certificate (detail)**
- **show security pki certificate-request (detail)**
- **show security pki local-certificate (detail)**

The following sections show the output of these commands used with the configuration example:

- [Router 1 on page 155](#)
- [Router 2 on page 156](#)
- [Router 3 on page 160](#)
- [Router 4 on page 163](#)

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface on Router 4 to send traffic across the IPsec tunnel.

```
user@R1> ping 10.1.56.2
```

```
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=254 time=1.351 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=254 time=1.187 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=254 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=254 time=1.154 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=254 time=1.156 ms
^C
--- 10.1.56.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.154/1.204/1.351/0.074 ms
```

If you ping the loopback address of Router 4, the operation succeeds because the address is part of the OSPF network configured on Router 4.

```
user@R1> ping 10.0.0.4

PING 10.0.0.4 (10.0.0.4): 56 data bytes
64 bytes from 10.0.0.4: icmp_seq=0 ttl=62 time=1.318 ms
64 bytes from 10.0.0.4: icmp_seq=1 ttl=62 time=1.084 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=62 time=3.260 ms
^C
--- 10.0.0.4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.084/1.887/3.260/0.975 ms
```

Router 2

To verify that matched traffic is being diverted to the bidirectional IPsec tunnel, view the IPsec statistics:

```
user@R2> show services ipsec-vpn ipsec statistics

PIC: sp-1/2/0, Service set: service-set-dynamic-BiEspsha3des

ESP Statistics:
  Encrypted bytes:      162056
  Decrypted bytes:      161896
  Encrypted packets:    2215
  Decrypted packets:    2216
AH Statistics:
  Input bytes:          0
  Output bytes:         0
  Input packets:        0
  Output packets:       0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations** command:

```
user@R2> show services ipsec-vpn ike security-associations
```


Remote Address	State	Initiator cookie	Responder cookie	Exchange type
10.1.15.2	Matured	d82610c59114fd37	ec4391f76783ef28	Main

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the default settings inherent in the AS PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: service-set-dynamic-BiEspsha3des
```

```
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
IPSec inside interface: sp-1/2/0.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

Direction: inbound, SPI: 857451461, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 9052 seconds
Hard lifetime: Expires in 9187 seconds
Anti-replay service: Enabled, Replay window size: 64

Direction: outbound, SPI: 1272330309, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 9052 seconds
Hard lifetime: Expires in 9187 seconds
Anti-replay service: Enabled, Replay window size: 64
```

To display the digital certificates that are used to establish the IPsec tunnel, issue the **show services ipsec-vpn certificates** command:

```
user@R2> show services ipsec-vpn certificates
```

```
Service set: service-set-dynamic-BiEspsha3des, Total entries: 3
```

```
Certificate cache entry: 3
Flags: Non-root Trusted
Issued to: router3.example.com, Issued by: juniper
Alternate subject: router3.example.com
Validity:
  Not before: 2005 Nov 21st, 23:33:58 GMT
  Not after: 2008 Nov 22nd, 00:03:58 GMT
```

```
Certificate cache entry: 2
Flags: Non-root Trusted
Issued to: router2.example.com, Issued by: juniper
Alternate subject: router2.example.com
Validity:
  Not before: 2005 Nov 21st, 23:28:22 GMT
  Not after: 2008 Nov 21st, 23:58:22 GMT
```

```
Certificate cache entry: 1
Flags: Root Trusted
Issued to: juniper, Issued by: juniper
```

```

Validity:
  Not before: 2005 Oct 18th, 23:54:22 GMT
  Not after: 2025 Oct 19th, 00:24:22 GMT

```

To display the CA certificate, issue the **show security pki ca-certificate detail** command. Notice that there are three separate certificates: one for certificate signing, one for key encipherment, and one for the CA's digital signature.

```
user@R2> show security pki ca-certificate detail
```

```

Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 9235
Issuer:
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us
Validity:
  Not before: 2005 Oct 18th, 23:54:22 GMT
  Not after: 2025 Oct 19th, 00:24:22 GMT
Public key algorithm: rsaEncryption(1024 bits)
cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
04:47:08:07:de:17:23:13
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
  71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
Distribution CRL:
  C=us, O=juniper, CN=CRL1
  http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: CRL signing, Certificate signing

Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925c
Issuer:
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us, Common name: First Officer
Validity:
  Not before: 2005 Oct 18th, 23:55:59 GMT
  Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
da:eb:10:27:bd:46:34:33
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
  23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)

```

```

Distribution CRL:
  C=us, O=juniper, CN=CRL1
  http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: Key encipherment
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925b
Issuer:
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us, Common name: First Officer
Validity:
  Not before: 2005 Oct 18th, 23:55:59 GMT
  Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
  ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
  d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
  00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
  e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
  90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
  b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
  af:44:bf:53:aa:d4:5f:67
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
  ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
Distribution CRL:
  C=us, O=juniper, CN=CRL1
  http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: Digital signature

```

To display the local certificate request, issue the **show security pki certificate-request** command:

```

user@R2> show security pki certificate-request
Certificate identifier: local-entrust2
  Issued to: router2.example.com
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed

```

To display the local certificate, issue the **show security pki local-certificate** command:

```

user@R2> show security pki local-certificate
Certificate identifier: local-entrust2
  Issued to: router2.example.com, Issued by: juniper
  Validity:
    Not before: 2005 Nov 21st, 23:28:22 GMT
    Not after: 2008 Nov 21st, 23:58:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed

```

Router 3

To verify that matched traffic is being diverted to the bidirectional IPsec tunnel, view the IPsec statistics:

```
user@R3> show services ipsec-vpn ipsec statistics
```

```
PIC: sp-1/2/0, Service set: service-set-dynamic-BiEspsha3des
```

ESP Statistics:

```
Encrypted bytes:      161896
Decrypted bytes:      162056
Encrypted packets:    2216
Decrypted packets:    2215
```

AH Statistics:

```
Input bytes:          0
Output bytes:         0
Input packets:        0
Output packets:       0
```

Errors:

```
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ike security-associations
```

Remote Address	State	Initiator cookie	Responder cookie	Exchange type
10.1.15.1	Matured	d82610c59114fd37	ec4391f76783ef28	Main

To verify that the IPsec SA is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: service-set-dynamic-BiEspsha3des
```

```
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
IPsec inside interface: sp-1/2/0.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Direction: inbound, SPI: 1272330309, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 7219 seconds
Hard lifetime: Expires in 7309 seconds
Anti-replay service: Enabled, Replay window size: 64
```

```
Direction: outbound, SPI: 857451461, AUX-SPI: 0
```

```

Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 7219 seconds
Hard lifetime: Expires in 7309 seconds
Anti-replay service: Enabled, Replay window size: 64

```

To display the digital certificates that are used to establish the IPsec tunnel, issue the **show services ipsec-vpn certificates** command:

```

user@R3> show services ipsec-vpn certificates
Service set: service-set-dynamic-BiEspsha3des, Total entries: 3
Certificate cache entry: 3
  Flags: Non-root Trusted
  Issued to: router3.example.com, Issued by: juniper
  Alternate subject: router3.example.com
  Validity:
    Not before: 2005 Nov 21st, 23:33:58 GMT
    Not after: 2008 Nov 22nd, 00:03:58 GMT

Certificate cache entry: 2
  Flags: Non-root Trusted
  Issued to: router2.example.com, Issued by: juniper
  Alternate subject: router2.example.com
  Validity:
    Not before: 2005 Nov 21st, 23:28:22 GMT
    Not after: 2008 Nov 21st, 23:58:22 GMT

Certificate cache entry: 1
  Flags: Root Trusted
  Issued to: juniper, Issued by: juniper
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT

```

To display the CA certificate, issue the **show security pki ca-certificate detail** command. Notice that there are three separate certificates: one for certificate signing, one for key encipherment, and one for the CA's digital signature.

```

user@R3> show security pki ca-certificate detail
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 9235
Issuer:
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us
Validity:
  Not before: 2005 Oct 18th, 23:54:22 GMT
  Not after: 2025 Oct 19th, 00:24:22 GMT
Public key algorithm: rsaEncryption(1024 bits)
cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2

```

```
c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
04:47:08:07:de:17:23:13
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
  71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
Distribution CRL:
  C=us, O=juniper, CN=CRL1
  http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: CRL signing, Certificate signing
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925c
Issuer:
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us, Common name: First Officer
Validity:
  Not before: 2005 Oct 18th, 23:55:59 GMT
  Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
da:eb:10:27:bd:46:34:33
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
  23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
Distribution CRL:
  C=us, O=juniper, CN=CRL1
  http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Key encipherment
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925b
Issuer:
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us, Common name: First Officer
Validity:
  Not before: 2005 Oct 18th, 23:55:59 GMT
  Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
af:44:bf:53:aa:d4:5f:67
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
  ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
Distribution CRL:
  C=us, O=juniper, CN=CRL1
```

```
http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Digital signature
```

To display the local certificate request, issue the **show security pki certificate-request** command:

```
user@R3> show security pki certificate-request
Certificate identifier: local-entrust3
  Issued to: router3.example.com
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

To display the local certificate, issue the **show security pki local-certificate** command:

```
user@R3> show security pki local-certificate
Certificate identifier: local-entrust3
  Issued to: router3.example.com, Issued by: juniper
  Validity:
    Not before: 2005 Nov 21st, 23:33:58 GMT
    Not after: 2008 Nov 22nd, 00:03:58 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface on Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms
```

The final way you can confirm that traffic travels over the IPsec tunnel is by issuing the **traceroute** command to the **so-0/0/0** interface on Router 1. Notice that the physical interface between Routers 2 and 3 is not referenced in the path; traffic enters the IPsec tunnel through the adaptive services IPsec inside interface on Router 3, passes through the loopback interface on Router 2, and ends at the **so-0/0/0** interface on Router 1.

```
user@R4> traceroute 10.1.12.2
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1  10.1.15.2 (10.1.15.2)  0.987 ms  0.630 ms  0.563 ms
 2  10.0.0.2 (10.0.0.2)  1.194 ms  1.058 ms  1.033 ms
 3  10.1.12.2 (10.1.12.2)  1.073 ms  0.949 ms  0.932 ms
```

For additional information on using digital certificates, see the *Junos Services Interfaces Configuration Guide* and the *Junos System Basics and Services Command Reference*.

Example: Dynamic Endpoint Tunneling Configuration

Figure 10: IPSec Dynamic Endpoint Tunneling Topology Diagram

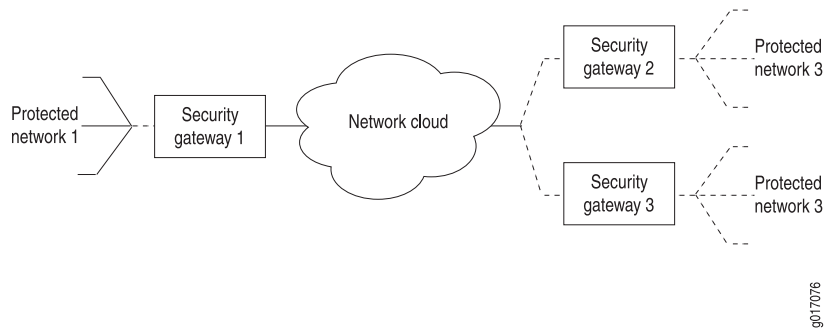


Figure 10 on page 164 shows a local network N-1 located behind security gateway SG-1. SG-1 is a Juniper Networks router terminating dynamic peer endpoints. The tunnel termination address on SG-1 is 10.7.7.2 and the local network address is 172.16.1.0/24.

A remote peer router obtains addresses from an ISP pool and runs RFC-compliant IKE. Remote network N-2 has address 172.16.2.0/24 and is located behind security gateway SG-2 with tunnel termination address 10.7.7.1.

On Router SG-1, configure an IKE access profile to accept proposals from SG-2. Apply the interface identifier from the access profile to the inside services interface and apply the IKE access profile itself to the IPSec next-hop style service set.

Router SG-1

```
[edit]
access {
  profile ike_access {
    client * { # Accepts proposals from specified peers that use the preshared key.
      ike {
        allowed-proxy-pair local 10.255.14.63/32 remote 10.255.14.64/32;
        pre-shared-key ascii-text "$ABC123"; # SECRET-DATA
        interface-id test_id; # Apply this ID to the inside services interfaces.
      }
    }
  }
}
interfaces {
  fe-0/0/0 {
    description "Connection to the local network";
    unit 0 {
      family inet {
        address 172.16.1.1/24;
      }
    }
  }
  so-1/0/0 {
```



```

description "Connection to SG-2";
no-keepalives;
encapsulation cisco-hdlc;
unit 0 {
    family inet {
        address 10.7.7.2/30;
    }
}
}
sp-3/3/0 {
    unit 0 {
        family inet;
    }
    unit 3 {
        dial-options {
            ipsec-interface-id test_id; # Accepts dynamic endpoint tunnels.
            shared;
        }
        service-domain inside;
    }
    unit 4 {
        family inet;
        service-domain outside;
    }
}
}
services {
    service-set dynamic_nh_ss { # Create a next-hop service set
        next-hop-service { # for the dynamic endpoint tunnels.
            inside-service-interface sp-3/3/0.3;
            outside-service-interface sp-3/3/0.4;
        }
        ipsec-vpn-options {
            local-gateway 10.7.7.2;
            ike-access-profile ike_access; # Apply the IKE access profile here.
        }
    }
}
}

```

Verifying Your Work

To verify proper operation of a dynamic endpoint tunnel configured on the AS PIC, use the following command:

```
show services ipsec-vpn ipsec security-associations (detail)
```

The following section shows output from this command used with the configuration example. The dynamically created rule `_junos_` appears in the output, as well as the establishment of the inbound and outbound dynamically created tunnels.

```
user@router> show services ipsec-vpn ipsec security-associations detail
```

Service set: dynamic_nh_ss

Rule: _junos_ , Term: tunnel4, Tunnel index: 4
Local gateway: 10.7.7.2, Remote gateway: 10.7.7.1
Local identity: ipv4(any:0,[0..3]=10.255.14.63)
Remote identity: ipv4(any:0,[0..3]=10.255.14.64)

Direction: inbound , SPI: 428111023, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 27660 seconds
Hard lifetime: Expires in 27750 seconds
Anti-replay service: Enabled, Replay window size: 64

Direction: outbound , SPI: 4035429231, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 27660 seconds
Hard lifetime: Expires in 27750 seconds
Anti-replay service: Enabled, Replay window size: 64

PART 3

Digital Certificates

- [Configuring Digital Certificates on page 169](#)
- [Configuring SSH and SSL Router Access on page 207](#)

CHAPTER 9

Configuring Digital Certificates

- [Public Key Cryptography on page 169](#)
- [Configuring Digital Certificates on page 174](#)
- [Configuring Digital Certificates for an ES PIC on page 177](#)
- [IKE Policy for Digital Certificates on an ES PIC on page 182](#)
- [Configuring Digital Certificates for Adaptive Services Interfaces on page 185](#)
- [Configuring Auto-Reenrollment of a Router Certificate on page 194](#)
- [IPsec Tunnel Traffic Configuration on page 196](#)
- [Tracing Operations for Security Services on page 203](#)

Public Key Cryptography

- [Understanding Public Key Cryptography on Switches on page 170](#)
- [Understanding Self-Signed Certificates on EX Series Switches on page 171](#)
- [Manually Generating Self-Signed Certificates on Switches \(CLI Procedure\) on page 172](#)
- [Deleting Self-Signed Certificates \(CLI Procedure\) on page 173](#)
- [Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates \(CLI Procedure\) on page 173](#)

Understanding Public Key Cryptography on Switches

Cryptography describes the techniques related to the following aspects of information security:

- Privacy or confidentiality
- Integrity of data
- Authentication
- Nonrepudiation or nonrepudiation of origin—Nonrepudiation of origin means that signers cannot claim that they did not sign a message while claiming that their private key remains secret. In some nonrepudiation schemes used in digital signatures, a timestamp is attached to the digital signature, so that even if the private key is exposed, the signature remains valid. Public and private keys are described in the following text.

In practice, cryptographic methods protect the data transferred from one system to another over public networks by encrypting the data using an encryption key. Public key cryptography (PKC), which is used on Juniper Networks EX Series Ethernet Switches, uses a pair of encryption keys: a public key and a private key. The public and private keys are created simultaneously using the same encryption algorithm. The private key is held by a user secretly and the public key is published. Data encrypted with a public key can be decrypted only with the corresponding private key and vice versa. When you generate a public/private key pair, the switch automatically saves the key pair in a file in the certificate store, from which it is subsequently used in certificate request commands. The generated key pair is saved as *certificate-id.priv*.



NOTE: The default RSA and DSA key size is 1024 bits. If you are using the Simple Certificate Enrollment Protocol (SCEP), Juniper Networks Junos operating system (Junos OS) supports RSA only.

- [Public Key Infrastructure \(PKI\) and Digital Certificates on page 170](#)

Public Key Infrastructure (PKI) and Digital Certificates

Public key infrastructure (PKI) allows the distribution and use of the public keys in public key cryptography with security and integrity. PKI manages the public keys by using digital certificates. A digital certificate provides an electronic means of verifying the identity of an individual, an organization, or a directory service that can store digital certificates.

A PKI typically consists of a Registration Authority (RA) that verifies the identities of entities, authorizes their certificate requests, and generates unique asymmetric key pairs (unless the users' certificate requests already contain public keys); and a Certificate Authority (CA) that issues corresponding digital certificates for the requesting entities. Optionally, you can use a Certificate Repository that stores and distributes certificates and a certificate revocation list (CRL) identifying the certificates that are no longer valid. Each entity possessing the authentic public key of a CA can verify the certificates issued by that CA.

Digital signatures exploit the public key cryptographic system as follows:

1. A sender digitally signs data by applying a cryptographic operation, involving its private key, on a digest of the data.
2. The resulting signature is attached to the data and sent to the receiver.
3. The receiver obtains the digital certificate of the sender, which provides the sender's public key and confirmation of the link between its identity and the public key. The sender's certificate is often attached to the signed data.
4. The receiver either trusts this certificate or attempts to verify it. The receiver verifies the signature on the data by using the public key contained in the certificate. This verification ensures the authenticity and integrity of the received data.

As an alternative to using a PKI, an entity can distribute its public key directly to all potential signature verifiers, so long as the key's integrity is protected. The switch does it by using a self-signed certificate as a container for the public key and the corresponding entity's identity.

See Also • [Understanding Self-Signed Certificates on EX Series Switches on page 171](#)

Understanding Self-Signed Certificates on EX Series Switches

When you initialize a Juniper Networks EX Series Ethernet Switch with the factory default configuration, the switch generates a self-signed certificate, allowing secure access to the switch through the Secure Sockets Layer (SSL) protocol. Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) and XML Network Management over Secure Sockets Layer (XNM-SSL) are the two services that can make use of the self-signed certificates.



NOTE: Self-signed certificates do not provide additional security as do those generated by Certificate Authorities (CAs). This is because a client cannot verify that the server he or she has connected to is the one advertised in the certificate.

The switches provide two methods for generating a self-signed certificate:

- Automatic generation

In this case, the creator of the certificate is the switch. An automatically generated (also called "system-generated") self-signed certificate is configured on the switch by default.

After the switch is initialized, it checks for the presence of an automatically generated self-signed certificate. If it does not find one, the switch generates one and saves it in the file system.

A self-signed certificate that is automatically generated by the switch is similar to an SSH host key. It is stored in the file system, not as part of the configuration. It persists when the switch is rebooted, and it is preserved when a **request system snapshot** command is issued.

The switch uses the following distinguished name for the automatically generated certificate:

"CN=<device serial number>, CN=system generated, CN=self-signed"

If you delete the system-generated self-signed certificate on the switch, the switch generates a self-signed certificate automatically.

- Manual generation

In this case, you create the self-signed certificate for the switch. At any time, you can use the CLI to generate a self-signed certificate. Manually generated self-signed certificates are stored in the file system, not as part of the configuration.

Self-signed certificates are valid for five years from the time they are generated. When the validity of an automatically generated self-signed certificate expires, you can delete it from the switch so that the switch generates a new self-signed certificate.

System-generated self-signed certificates and manually generated self-signed certificates can coexist on the switch.

Manually Generating Self-Signed Certificates on Switches (CLI Procedure)

EX Series switches allow you to generate custom self-signed certificates and store them in the file system. The certificate you generate manually can coexist with the automatically generated self-signed certificate on the switch. To enable secure access to the switch over SSL, you can use either the system-generated self-signed certificate or a certificate you have generated manually.

To generate self-signed certificates manually, you must complete the following tasks:

- [Generating a Public-Private Key Pair on Switches on page 172](#)
- [Generating Self-Signed Certificates on Switches on page 173](#)

Generating a Public-Private Key Pair on Switches

A digital certificate has an associated cryptographic key pair that is used to sign the certificate digitally. The cryptographic key pair comprises a public key and a private key. When you generate a self-signed certificate, you must provide a public-private key pair that can be used to sign the self-signed certificate. Therefore, you must generate a public-private key pair before you can generate a self-signed certificate.

To generate a public-private key pair:

```
user@switch> request security pki generate-key-pair certificate-id certificate-id-name
```



NOTE: Optionally, you can specify the encryption algorithm and the size of the encryption key. If you do not specify the encryption algorithm and encryption key size, default values are used. The default encryption algorithm is RSA, and the default encryption key size is 1024 bits.

After the public-private key pair is generated, the switch displays the following:

generated key pair *certificate-id-name*, key size 1024 bits

Generating Self-Signed Certificates on Switches

To generate the self-signed certificate manually, include the certificate ID name, the subject of the distinguished name (DN), the domain name, the IP address of the switch, and the e-mail address of the certificate holder:

```
user@switch> request security pki local-certificate generate-self-signed certificate-id
certificate-id-name domain-name domain-name email email-address ip-address switch-ip-address
subject subject-of-distinguished-name
```

The certificate you have generated is stored in the switch's file system. The certificate ID you have specified while generating the certificate is a unique identifier that you can use to enable the HTTPS or XNM-SSL services.

To verify that the certificate was generated and loaded properly, enter the **show security pki local-certificate** operational command.

See Also • [Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates \(CLI Procedure\) on page 173](#)

Deleting Self-Signed Certificates (CLI Procedure)

You can delete a self-signed certificate that is automatically or manually generated from the EX Series switch. When you delete the automatically generated self-signed certificate, the switch generates a new self-signed certificate and stores it in the file system.

- To delete the automatically generated certificate and its associated key pair from the switch:

```
user@switch> clear security pki local-certificate system-generated
```

- To delete a manually generated certificate and its associated key pair from the switch:

```
user@switch> clear security pki local-certificate certificate-id certificate-id-name
```

- To delete all manually generated certificates and their associated key pairs from the switch:

```
user@switch> clear security pki local-certificate all
```

Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)

You can use the system-generated self-signed certificate or a manually generated self-signed certificate to enable Web management HTTPS and XNM-SSL services.

- To enable HTTPS services using the automatically generated self-signed certificate:

```
[edit]
```

```
user@switch# set system services web-management https system-generated-certificate
```

- To enable HTTPS services using a manually generated self-signed certificate:

```
[edit]
user@switch# set system services web-management https pki-local-certificate
certificate-id-name
```



NOTE: The value of the *certificate-id-name* must match the name you specified when you generated the self-signed certificate manually.

- To enable XNM-SSL services using a manually generated self-signed certificate:

```
[edit]
user@switch# set system services xnm-ssl local-certificate certificate-id-name
```



NOTE: The value of the *certificate-id-name* must match the name you specified when you generated the self-signed certificate manually.

- See Also**
- [Manually Generating Self-Signed Certificates on Switches \(CLI Procedure\) on page 172](#)
 - [Understanding Self-Signed Certificates on EX Series Switches on page 171](#)

Configuring Digital Certificates

- [Digital Certificates Overview on page 174](#)
- [Obtaining a Certificate from a Certificate Authority for an ES PIC on page 175](#)
- [Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router on page 175](#)
- [Example: Requesting a CA Digital Certificate on page 176](#)
- [Generating a Private and Public Key Pair for Digital Certificates for an ES PIC on page 176](#)

Digital Certificates Overview

A digital certificate provides a way of authenticating users through a trusted third-party called a certificate authority (CA). The CA validates the identity of a certificate holder and “signs” the certificate to attest that it has not been forged or altered.

A certificate includes the following information:

- The distinguished name (DN) of the owner. A DN is a unique identifier and consists of a fully qualified name including the common name (CN) of the owner, the owner’s organization, and other distinguishing information.
- The public key of the owner.
- The date on which the certificate was issued.

- The date on which the certificate expires.
- The distinguished name of the issuing CA.
- The digital signature of the issuing CA.

The additional information in a certificate allows recipients to decide whether to accept the certificate. The recipient can determine if the certificate is still valid based on the expiration date. The recipient can check whether the CA is trusted by the site based on the issuing CA.

With a certificate, a CA takes the owner's public key, signs that public key with its own private key, and returns this to the owner as a certificate. The recipient can extract the certificate (containing the CA's signature) with the owner's public key. By using the CA's public key and the CA's signature on the extracted certificate, the recipient can validate the CA's signature and owner of the certificate.

When you use digital certificates, your first step is to send a request to obtain a certificate from your CA. You then configure digital certificates and a digital certificate IKE policy. Finally, you obtain a digitally signed certificate from a CA.



NOTE: Certificates without an alternate subject name are not appropriate for IPsec services.

Obtaining a Certificate from a Certificate Authority for an ES PIC

Certificate authorities (CAs) manage certificate requests and issue certificates to participating IPsec network devices. When you create a certificate request, you need to provide the information about the owner of the certificate. The required information and its format vary across certificate authorities.

Certificates use names in the X.500 format, a directory access protocol that provides both read and update access. The entire name is called a DN (distinguished name). It consists of a set of components, which often includes a CN (common name), an organization (O), an organization unit (OU), a country (C), a locality (L), and so on.



NOTE: For the dynamic registration of digital certificates, the Junos OS supports only the Simple Certificate Enrollment Protocol (SCEP).

See Also • [Digital Certificates Overview on page 174](#)

Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router

For an encryption interface on an M Series or T Series router, issue the following command to obtain a public key certificate from a CA. The results are saved in the specified file in the `/var/etc/ikecert` directory. The CA public key verifies certificates from remote peers.

```
user@host> request security certificate enroll filename filename ca-name ca-name
parameters parameters
```

- See Also**
- [Example: Requesting a CA Digital Certificate on page 176](#)
 - [Digital Certificates Overview on page 174](#)

Example: Requesting a CA Digital Certificate

Specify a URL to the SCEP server and the name of the certification authority whose certificate you want: **mycompany.com**. **filename** is name of the file that stores the result. The output, "Received CA certificate:" provides the signature for the certificate, which allows you to verify (offline) that the certificate is genuine.

```
user@host> request security certificate enroll filename ca_verisign ca-file verisign ca-name
xyzcompany url
http://hostname/path/filename
URL: http://hostname/path/filename name: example.com CA file: verisign Encoding: binary
Certificate enrollment has started. To see the certificate enrollment status, check the key
management process (kmd) log file at /var/log/kmd. <-----
```



NOTE: Each router is initially manually enrolled with a certificate authority.

- See Also**
- [Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router on page 175](#)

Generating a Private and Public Key Pair for Digital Certificates for an ES PIC

To generate a private and public key, issue the following command:

```
user@host> request security key-pair name size key-size type ( rsa | dsa )
```

name specifies the filename in which to store the public and private keys.

key-size can be 512, 1024, 1596, or 2048 bytes. The default key size is 1024 bytes.

type can be **rsa** or **dsa**. The default is RSA.



NOTE: When you use SCEP, the Junos OS only supports RSA.

The following example shows how to generate a private and public key pair:

```
user@host> request security key-pair batt
Generated key pair, key size 1024, file batt Algorithm RSA
```

- See Also**
- [Digital Certificates Overview on page 174](#)

Configuring Digital Certificates for an ES PIC

Digital certificates provide a way of authenticating users through a trusted third party called a certificate authority (CA). The CA validates the identity of a certificate holder and “signs” the certificate to attest that it has not been forged or altered.

To define the digital certificate configuration for an encryption service interface, include the following statements at the **[edit security certificates]** and **[edit security ike]** hierarchy levels:

```
[edit security]
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl filename;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-filename {
    certificate-key-string;
    load-key-file URL key-file-name;
  }
  maximum-certificates number;
  path-length certificate-path-length;
}
ike {
  policy ike-peer-address {
    description policy;
    encoding (binary | pem);
    identity identity-name;
    local-certificate certificate-filename;
    local-key-pair private-public-key-file;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
  }
}
```

Tasks to configure digital certificates for ES PICs are:

- [Configuring the Certificate Authority Properties for an ES PIC on page 178](#)
- [Configuring the Cache Size on page 180](#)
- [Configuring the Negative Cache on page 180](#)
- [Configuring the Number of Enrollment Retries on page 180](#)
- [Configuring the Maximum Number of Peer Certificates on page 181](#)
- [Configuring the Path Length for the Certificate Hierarchy on page 181](#)

Configuring the Certificate Authority Properties for an ES PIC

A CA is a trusted third-party organization that creates, enrolls, validates, and revokes digital certificates.

To configure a certificate authority and its properties for an ES PIC, include the following statements at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
certification-authority ca-profile-name {
  ca-name ca-identity;
  crl filename;
  encoding (binary | pem);
  enrollment-url url-name;
  file certificate-filename;
  ldap-url url-name;
}
```

ca-profile-name is the CA profile name.

Tasks for configuring the CA properties are:

1. [Specifying the Certificate Authority Name on page 178](#)
2. [Configuring the Certificate Revocation List on page 178](#)
3. [Configuring the Type of Encoding Your CA Supports on page 179](#)
4. [Specifying an Enrollment URL on page 179](#)
5. [Specifying a File to Read the Digital Certificate on page 179](#)
6. [Specifying an LDAP URL on page 179](#)

Specifying the Certificate Authority Name

If you are enrolling with a CA using simple certificate enrollment protocols (SCEP), you need to specify the CA name (CA identity) that is used in the certificate request, in addition to the URL for the SCEP server.

To specify the name of the CA identity, include the **ca-name** statement at the **[edit security certificates certification-authority *ca-profile-name*]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
ca-name ca-identity;
```

ca-identity specifies the CA identity to use in the certificate request. It is typically the CA domain name.

Configuring the Certificate Revocation List

A certificate revocation list (CRL) contains a list of digital certificates that have been canceled before their expiration date. When a participating peer uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL.

To configure the CA certificate revocation list, include the **crl** statement and specify the file from which to read the CRL at the **[edit security certificates certification-authority ca-profile-name]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
crl filename;
```

Configuring the Type of Encoding Your CA Supports

By default, encoding is set to binary. Encoding specifies the file format used for the **local-certificate** and **local-key-pair** statements. By default, the binary (distinguished encoding rules) format is enabled. Privacy-enhanced mail (PEM) is an ASCII base 64 encoded format. Check with your CA to determine which file formats it supports.

To configure the file format that your CA supports, include the **encoding** statement and specify a binary or PEM format at the **[edit security certificates certification-authority ca-profile-name]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
encoding (binary | pem);
```

Specifying an Enrollment URL

You specify the CA location where your router or switch sends SCEP-based certificate enrollment requests. To specify the CA location by naming the CA URL, include the **enrollment-url** statement at the **[edit security certificates certification-authority ca-profile-name]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
enrollment-url url-name;
```

url-name is the CA location. The format is **http://ca-name**, where **ca-name** is the CA host DNS name or IP address.

Specifying a File to Read the Digital Certificate

To specify the file from which to read the digital certificate, include the **file** statement and specify the certificate filename at the **[edit security certificates certification-authority ca-profile-name]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
file certificate-filename;
```

Specifying an LDAP URL

If your CA stores its current CRL at its Lightweight Directory Access Protocol (LDAP) server, you can optionally check your CA CRL list before using a digital certificate. If the digital certificate appears on the CA CRL, your router or switch cannot use it. To access your CA CRL, include the **ldap-url** statement at the **[edit security certificates certification-authority ca-profile-name]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]  
  ldap-url url-name;
```

url-name is the certification authority LDAP server name. The format is `ldap://server-name`, where *server-name* is the CA host DNS name or IP address.

Configuring the Cache Size

By default, the cache size is 2 megabytes (MB). To configure total cache size for digital certificates, include the `cache-size` statement at the `[edit security certificates]` hierarchy level:

```
[edit security certificates]  
  cache-size bytes;
```

bytes is the cache size for digital certificates. The range can be from 64 through 4,294,967,295 bytes.



NOTE: We recommend that you limit your cache size to 4 MB.

Configuring the Negative Cache

Negative caching stores negative results and reduces the response time for negative answers. It also reduces the number of messages that are sent to the remote server. Maintaining a negative cache state allows the system to quickly return a failure condition when a lookup attempt is retried. Without a negative cache state, a retry would require waiting for the remote server to fail to respond, even though the system already “knows” that remote server is not responding.

By default, the negative cache is 20 seconds. To configure the negative cache, include the `cache-timeout-negative` statement at the `[edit security certificates]` hierarchy level:

```
[edit security certificates]  
  cache-timeout-negative seconds;
```

seconds is the amount of time for which a failed CA or router certificate is present in the negative cache. While searching for certificates with a matching CA identity (domain name for certificates or CA domain name and serial for CRLs), the negative cache is searched first. If an entry is found in the negative cache, the search fails immediately.



NOTE: Configuring a large negative cache value can make you susceptible to a denial-of-service (DoS) attack.

Configuring the Number of Enrollment Retries

By default, the number of enrollment retries is set to 0, an infinite number of retries. To specify how many times a router or switch will resend a certificate request, include the `enrollment-retry` statement at the `[edit security certificates]` hierarchy level:


```
[edit security certificates]
enrollment-retry attempts;
```

attempts is the number of enrollment retries (0 through 100).

Configuring the Maximum Number of Peer Certificates

By default, the maximum number of peer certificates to be cached is 1024. To configure the maximum number of peer certificates to be cached, include the **maximum-certificates** statement at the **[edit security certificates]** hierarchy statement level:

```
[edit security certificates]
maximum-certificates number;
```

number is the maximum number of peer certificates to be cached. The range is from 64 through 4,294,967,295 peer certificates.

Configuring the Path Length for the Certificate Hierarchy

Certification authorities can issue certificates to other CAs. This creates a tree-like certification hierarchy. The highest trusted CA in the hierarchy is called the *trust anchor*. Sometimes the trust anchor is the root CA, which is usually signed by itself. In the hierarchy, every certificate is signed by the CA immediately above it. An exception is the root CA certificate, which is usually signed by the root CA itself. In general, a chain of multiple certificates may be needed, comprising a certificate of the public key owner (the end entity) signed by one CA, and zero or more additional certificates of CAs signed by other CAs. Such chains, called certification paths, are required because a public key user is only initialized with a limited number of assured CA public keys.

Path length refers to a path of certificates from one certificate to another certificate, based on the relationship of a CA and its “children.” When you configure the **path-length** statement, you specify the maximum depth of the hierarchy to validate a certificate from the trusted root CA certificate to the certificate in question. For more information about the certificate hierarchy, see RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

By default, the maximum certificate path length is set to 15. The root anchor is 1.

To configure path length, include the **path-length** statement at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
path-length certificate-path-length;
```

certificate-path-length is the maximum number certificates for the certificate path length. The range is from 2 through 15 certificates.

- See Also**
- [Configuring an IKE Policy for Digital Certificates for an ES PIC on page 182](#)
 - [Digital Certificates Overview on page 174](#)
 - [Configuring Digital Certificates for Adaptive Services Interfaces on page 185](#)

IKE Policy for Digital Certificates on an ES PIC

- [Configuring an IKE Policy for Digital Certificates for an ES PIC on page 182](#)
- [Obtaining a Signed Certificate from the CA for an ES PIC on page 183](#)
- [Associating the Configured Security Association with a Logical Interface on page 184](#)

Configuring an IKE Policy for Digital Certificates for an ES PIC

An IKE policy for digital certificates defines a combination of security parameters (IKE proposals) to be used during IKE negotiation. It defines a peer address and the proposals needed for that connection. During the IKE negotiation, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

To configure an IKE policy for digital certificates for an ES PIC, include the following statements at the `[edit security ike policy ike-peer-address]` hierarchy level:

```
[edit security ike]
policy ike-peer-address{
  encoding (binary | pem);
  identity identity-name;
  local-certificate certificate-filename;
  local-key-pair private-public-key-file;
}
```

Tasks for configuring an IKE policy for digital certificates are:

1. [Configuring the Type of Encoding Your CA Supports on page 182](#)
2. [Configuring the Identity to Define the Remote Certificate Name on page 182](#)
3. [Specifying the Certificate Filename on page 183](#)
4. [Specifying the Private and Public Key File on page 183](#)

Configuring the Type of Encoding Your CA Supports

By default, the encoding is set to binary. Encoding specifies the file format used for the **local-certificate** and **local-key-pair** statements. By default, the binary (distinguished encoding rules) format is enabled. PEM is an ASCII base 64 encoded format. Check with your CA to determine which file formats it supports.

To configure the file format that your CA supports, include the **encoding** statement and specify a binary or PEM format at the `[edit security ike policy ike-peer-address]` hierarchy level:

```
[edit security ike policy ike-peer-address ]
encoding (binary | pem);
```

Configuring the Identity to Define the Remote Certificate Name

To define the remote certificate name, include the **identity** statement at the `[edit security ike policy ike-peer-address]` hierarchy level:

```
[edit security ike policy ike-peer-address]
identity identity-name;
```

identity-name defines the identity of the remote certificate name if the identity cannot be learned through IKE (ID payload or IP address).

Specifying the Certificate Filename

To configure the certificate filename from which to read the local certificate, include the **local-certificate** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address]
local-certificate certificate-filename;
```

certificate-filename specifies the file from which to read the local certificate.

Specifying the Private and Public Key File

To specify the filename from which to read the public and private key, include the **local-key-pair** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address]
local-key-pair private-public-key-file;
```

private-public-key-file specifies the file from which to read the pair key.

See Also • [Digital Certificates Overview on page 174](#)

Obtaining a Signed Certificate from the CA for an ES PIC

To obtain a signed certificate from the CA, issue the following command:

```
user@host> request security certificate enroll filename filename subject c=us,o=x
alternative-subject certificate-ip-address certification-authority certificate-authority
key-file key-file-name domain-name domain-name
```

The results are saved in a specified file to the **/var/etc/ikecert** directory.

The following example shows how to obtain a CA signed certificate by referencing the configured **certification-authority** statement **local**. This statement is referenced by the **request security certificate enroll filename *filename* subject *subject* alternative-subject *alternative-subject* certification-authority *certification-authority*** command.

```
[edit]
security {
  certificates {
    certification-authority local {
      ca-name xyz.company.com;
      file l;
      enrollment-url "http://www.xyzcompany.com";
    }
  }
}
```

```
}
```

To obtain a signed certificate from the CA, issue the following command:

```
user@host> request security certificate enroll filename l subject c=uk,o=london
alternative-subject 10.50.1.4 certification-authority verisign key-file host-1.prv
domain-name host.xyzcompany.com
CA name: xyz.company.com CA file: ca_verisign
local pub/private key pair: host.prv
subject: c=uk,o=london domain name: host.example.com
alternative subject: 10.50.1.4
Encoding: binary
Certificate enrollment has started. To see the certificate enrollment status, check the key
management process (kmd) log file at /var/log/kmd. <-----
```

For information about how to use the operational mode commands to obtain a signed certificate, see the [CLI Explorer](#).

Another way to obtain a signed certificate from the CA is to reference the configured statements such as the URL, CA name, and CA certificate file by means of the **certification-authority** statement:

```
user@host> request security certificate enroll filename m subject c=us,o=x
alternative-subject 192.0.2.1 certification-authority local key-file y domain-name
abc.company.com
```

See Also • [Digital Certificates Overview on page 174](#)

Associating the Configured Security Association with a Logical Interface

Configuring the ES PIC associates the configured SA with a logical interface. This configuration defines the tunnel itself (logical subunit, tunnel addresses, maximum transmission unit [MTU], optional interface addresses, and the name of the SA to apply to traffic).

The addresses configured as the tunnel source and destination are the addresses in the outer IP header of the tunnel.



NOTE: The tunnel source address must be configured locally on the router, and the tunnel destination address must be a valid address for the security gateway terminating the tunnel.

The M5, M10, M20, and M40 routers support the ES PIC.

The SA must be a valid tunnel-mode SA. The interface address and destination address listed are optional. The destination address allows the user to configure a static route to encrypt traffic. If a static route uses that destination address as the next hop, traffic is forwarded through the portion of the tunnel in which encryption occurs.

The following example shows how to configure an IPsec tunnel as a logical interface on the ES PIC. The logical interface specifies the tunnel through which the encrypted traffic travels. The **ipsec-sa** statement associates the security profile with the interface.

```
[edit interfaces]
es-0/0/0 {
  unit 0 {
    tunnel {
      source tunnel 10.5.5.5; # tunnel source address
      destination 10.6.6.6; # tunnel destination address
    }
    family inet {
      ipsec-sa ipsec-sa; # name of security association to apply to packet
      address 10.1.1.8/32 { # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
    }
  }
}
```

See Also • [Configuring Security Associations for IPsec on an ES PIC on page 37](#)

Configuring Digital Certificates for Adaptive Services Interfaces

A digital certificate implementation uses the public key infrastructure (PKI), which requires that you generate a key pair consisting of a public key and a private key. The keys are created with a random number generator and are used to encrypt and decrypt data. In networks that do not use digital certificates, an IPsec-enabled device encrypts data with the private key and IPsec peers decrypt the data with the public key.

With digital certificates, the key sharing process requires an additional level of complexity. First, you and your IPsec peers request that a certificate authority (CA) send you a CA certificate that contains the public key of the CA. Next you request the CA to assign you a local digital certificate that contains the public key and some additional information. When the CA processes your request, it signs your local certificate with the private key of the CA. Then you install the CA certificate and the local certificate in your router and load the CA in remote devices before you can establish IPsec tunnels with your peers.



NOTE: For digital certificates, the Junos OS supports VeriSign, Entrust, Cisco Systems, and Microsoft Windows CAs for the Adaptive Services (AS) and Multiservices PICs.

To define digital certificates configuration for J Series Services Routers and AS and Multiservices PICs installed on M Series and T Series routers, include the following statements at the **[edit security pki]** hierarchy level:

```
[edit security]
pki {
  ca-profile ca-profile-name {
```

```

ca-identity ca-identity;
enrollment {
    url-name;
    retry number-of-enrollment-attempts;
    retry-interval seconds;
}
revocation-check {
    disable;
    crl {
        disable on-download-failure;
        refresh-interval number-of-hours;
        url {
            url-name;
            password;
        }
    }
}
}
}

```

The following tasks enable you to implement digital certificates on J Series Services Routers and AS and Multiservices PICs installed on M Series and T Series routers:

1. [Configuring the Certificate Authority Properties on page 186](#)
2. [Configuring the Certificate Revocation List on page 188](#)
3. [Managing Digital Certificates on page 189](#)
4. [Configuring Auto-Reenrollment of a Router Certificate on page 191](#)

Configuring the Certificate Authority Properties

A CA is a trusted third-party organization that creates, enrolls, validates, and revokes digital certificates.

To configure a certificate authority and its properties for the AS and Multiservices PICs, include the following statements at the **[edit security pki]** hierarchy level:

```

[edit security pki]
ca-profile ca-profile-name {
    ca-identity ca-identity;
    enrollment {
        url url-name;
        retry number-of-attempts;
        retry-interval seconds;
    }
}

```

Tasks for configuring the Certificate Authority properties are:

1. [Specifying the CA Profile Name on page 187](#)
2. [Specifying an Enrollment URL on page 187](#)
3. [Specifying the Enrollment Properties on page 187](#)

Specifying the CA Profile Name

The CA profile contains the name and URL of the CA or RA, as well as some retry-timer settings. CA certificates issued by Entrust, VeriSign, Cisco Systems, and Microsoft are compatible with the J Series Services Routers and AS and Multiservices PICs installed in the M Series and T Series routers.

To specify the CA profile name, include the **ca-profile statement** at the **[edit security pki]** security level:

```
[edit security pki]
ca-profile ca-profile-name;
```

You also need to specify the name of the CA identity used in the certificate request. This name is typically the domain name. To specify the name of the CA identity, include the **ca-identity statement** at the **[edit security pki ca-profile *ca-profile-name*]** level:

```
[edit security pki ca-profile ca-profile-name]
ca-identity ca-identity;
```

Specifying an Enrollment URL

You specify the CA location where your router should send the SCEP-based certificate enrollment requests. To specify the CA location by naming the CA URL, include the **url statement** at the **[edit security pki enrollment]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name enrollment]
url url-name;
```

url-name is the CA location. The format is **http://CA_name**, where **CA_name** is the CA host DNS name or IP address.

Specifying the Enrollment Properties

You can specify the number of times a router will resend a certificate request and the amount of time, in seconds, the router should wait between enrollment attempts.

By default, the number of enrollment retries is set to 0, an infinite number of retries. To specify how many times a router will resend a certificate request, include the **retry number-of-attempts statement** at the **[edit security pki ca-profile *ca-profile-name* enrollment]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name enrollment]
retry number-of-attempts;
```

The range for **number-of-attempts** is from 0 through 100.

To specify the amount of time, in seconds, that a router should wait between enrollment attempts, include the **retry-interval seconds statement** at the **[edit security pki ca-profile *ca-profile-name* enrollment]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name enrollment]
  retry-interval seconds;
```

The range for *seconds* is from 0 through 3600.

Configuring the Certificate Revocation List

Tasks to configure the certificate revocation list are:

1. [Specifying an LDAP URL on page 188](#)
2. [Configuring the Interval Between CRL Updates on page 189](#)
3. [Overriding Certificate Verification if CRL Download Fails on page 189](#)

Specifying an LDAP URL

You can specify the URL for the Lightweight Directory Access Protocol (LDAP) server where your CA stores its current CRL. If the CA includes the Certificate Distribution Point (CDP) in the digital certificate, you do not need to specify a URL for the LDAP server. The CDP is a field within the certificate that contains information about how to retrieve the CRL for the certificate. The router uses this information to download the CRL automatically.

Configure an LDAP URL if you want to use a different CDP from the one specified in the certificate. Any LDAP URL you configure takes precedence over the CDP included in the certificate.

You can configure up to three URLs for each CA profile.

If the LDAP server requires a password to access the CRL, you need to include the **password** statement.

To configure the router to retrieve the CRL from the LDAP server, include the **url** statement and specify the URL name at the **[edit security pki ca-profile ca-profile-name revocation-check crl]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl]
  url {
    url-name;
  }
```

url-name is the certificate authority LDAP server name. The format is **ldap://server-name**, where *server-name* is the CA host DNS name or IP address.

To specify to use a password to access the CRL, include the **password** statement at the **[edit security pki ca-profile ca-profile-name revocation-check crl url]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl url]
  password password;
```

password is the secret password that the LDAP server requires for access.

Configuring the Interval Between CRL Updates

By default, the time interval between CRL updates is 24 hours. To configure the amount of time between CRL updates, include the **refresh-interval** statement at the **[edit security pki ca-profile *ca-profile-name* revocation-check crl]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl]
refresh-interval number-of-hours;
```

The range for number of hours is from 0 through 8784.

Overriding Certificate Verification if CRL Download Fails

By default, if the router either cannot access the LDAP URL or retrieve a valid certificate revocation list, certificate verification fails and the IPsec tunnel is not established. To override this behavior and permit the authentication of the IPsec peer when the CRL is not downloaded, include the **disable on-download-failure** statement at the **[edit security pki ca-profile *ca-profile-name* revocation-check crl]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl]
disable on-download-failure;
```

Managing Digital Certificates

After you configure the CA profile, you can request a CA certificate from the trusted CA. Next, you must generate a public/private key pair. When the key pair is available, you can generate a local certificate either online or manually.

Tasks to manage digital certificates are:

1. [Requesting a CA Digital Certificate for AS and Multiservices PICs installed on M Series and T Series Routers on page 189](#)
2. [Generating a Public/Private Key Pair on page 190](#)
3. [Generating and Enrolling a Local Digital Certificate on page 190](#)

Requesting a CA Digital Certificate for AS and Multiservices PICs installed on M Series and T Series Routers

For J Series Services Routers and AS and Multiservices PICs installed on M Series and T Series routers, issue the following command to obtain a digital certificate from a CA. Specify a configured ***ca-profile-name*** to request a CA certificate from the trusted CA.

```
user@host>request security pki ca-certificate enroll ca-profile ca-profile-name
```

For information about how to configure a CA profile, see ["Configuring the Certificate Authority Properties" on page 186](#).

In this example, the certificate is enrolled online and installed into the router automatically.

```
user@host> request security pki ca-certificate enroll ca-profile entrust
```

Received following certificates:

Certificate: C=us, O=juniper

Fingerprint:00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10

Certificate: C=us, O=juniper, CN=First Officer

Fingerprint:bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17

Certificate: C=us, O=juniper, CN=First Officer

Fingerprint:46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f

Do you want to load the above CA certificate ? [yes,no] (no) yes



NOTE: If you obtain the CA certificate directly from the CA (for example, as an e-mail attachment or Web site download), you can install it with the **request security pki ca-certificate load** command. For more information, see the [CLI Explorer](#).

Generating a Public/Private Key Pair

After obtaining a certificate for an AS PIC or Multiservices PIC, you must generate a public-private key before you can generate a local certificate. The public key is included in the local digital certificate and the private key is used to decrypt data received from peers. To generate a public-private key pair, issue the **request security pki generate-key-pair certificate-id *certificate-id-name*** command.

The following example shows how to generate a public-private key for an AS PIC or Multiservices PIC:

```
user@host>request security pki generate-key-pair certificate-id local-entrust2
Generated key pair local-entrust2, key size 1024 bits
```

Generating and Enrolling a Local Digital Certificate

You can generate and enroll local digital certificates either online or manually. To generate and enroll a local certificate online by using the Simple Certificate Enrollment Protocol (SCEP) for an AS PIC or Multiservices PIC, issue the **request security pki local-certificate enroll** command. To generate a local certificate request manually in the PKCS-10 format, issue the **request security pki generate-certificate-request** command.

If you create the local certificate request manually, you must also load the certificate manually. To manually install a certificate in your router, issue the **request security pki local-certificate load** command.

The following example shows how to generate a local certificate request manually and send it to the CA for processing:

```
user@host> request security pki generate-certificate-request certificate-id local-entrust2
domain-name router2.example.com filename entrust-req2
```

```
subject cn=router2.example.com
```

Generated certificate request

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHAXLmp1bm1wZXIubmV0MIGfMAOGCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiuFk1Qws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8E1wTJ1kmIt2cB3yi fB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8o0Xyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjA0BgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHAXLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AA0BgQBc2rq1v5S0QXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtH406gQ3G
3iH0Zfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteo1ZCiZ70f09Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
```

```
-----END CERTIFICATE REQUEST-----
```

Fingerprint:

```
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

The trusted CA digitally signs the local certificate and returns it to you. Copy the certificate file into the router and load the certificate:

```
user@host> request security pki local-certificate load filename /tmp/router2-cert
certificate-id local-entrust2
Local certificate local-entrust2 loaded successfully
```



NOTE: The name of the file sent to you by the CA might not match the name of the certificate identifier. However, the **certificate-id** name must always match the name of the key pair you generated for the router.

After the local and CA certificates have been loaded, you can reference them in your IPsec configuration. Using default values in the AS and Multiservices PICs, you do not need to configure an IPsec proposal or an IPsec policy. However, you must configure an IKE proposal that specifies the use of digital certificates, reference the IKE proposal and locate the certificate in an IKE policy, and apply the CA profile to the service set.

Configuring Auto-Reenrollment of a Router Certificate

Use the **auto-re-enrollment** statement to configure automatic reenrollment of a specified existing router certificate before its existing expiration date. This function automatically reenrolls the router certificate. The reenrollment process requests the certificate authority (CA) to issue a new router certificate with a new expiration date. The date of auto-reenrollment is determined by the following parameters:

- **re-enroll-trigger-time**—The percentage of the difference between the router certificate start date/time (when the certificate was generated) and the validity period; used to specify how long auto-reenrollment should be initiated before expiration.
- **validity-period**—The number of days after issuance when the router certificate will expire, as set when a certificate is generated.



NOTE: By default, this feature is not enabled unless configured explicitly. This means that a certificate that does not have auto-reenrollment configured will expire on its normal expiration date.

The **ca-profile** statement specifies which CA will be contacted to reenroll the expiring certificate. This is the CA that issued the original router certificate.

The **challenge-password** statement provides the issuing CA with the router certificate's password, as set by the administrator and normally obtained from the SCEP enrollment Web page of the CA. The password is 16 characters in length.

Optionally, the router certificate key pair can be regenerated by using the **re-generate-keypair** statement.

To configure automatic reenrollment properties, include the following statements at the **[edit security pki]** hierarchy level:

```
[edit security pki]
auto-re-enrollment {
  certificate-id {
    ca-profile ca-profile-name;
    challenge-password password;
    re-enroll-trigger-time-percentage percentage;
    re-generate-keypair;
    validity-period days;
  }
}
```

percentage is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

days is the number of days for the validity period. The range can be from 1 through 4095.

Tasks to configure automatic reenrollment of certificates are:

1. [Specify the Certificate ID on page 192](#)
2. [Specify the CA Profile on page 193](#)
3. [Specify the Challenge Password on page 193](#)
4. [Specify the Reenroll Trigger Time on page 193](#)
5. [Specify the Regenerate Key Pair on page 193](#)
6. [Specify the Validity Period on page 194](#)

Specify the Certificate ID

Use the **certificate-id** statement to specify the name of the router certificate to configure for auto-reenrollment. To specify the certificate ID, include the statement at the **[edit security pki auto-re-enrollment]** hierarchy level:

```
[edit security pki auto-re-enrollment]
```

```
certificate-id certificate-name;
```

Specify the CA Profile

Use the **ca-profile** statement to specify the name of the CA profile from the router certificate previously specified by certificate ID. To specify the CA profile, include the statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
ca-profile ca-profile-name;
```



NOTE: The referenced **ca-profile** must have an enrollment URL configured at the **[edit security pki ca-profile *ca-profile-name* enrollment url]** hierarchy level.

Specify the Challenge Password

The challenge password is used by the CA specified by the PKI certificate ID for reenrollment and revocation. To specify the challenge password, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
challenge-password password;
```

Specify the Reenroll Trigger Time

Use the **re-enroll-trigger-time** statement to set the percentage of the validity period before expiration at which reenrollment occurs. To specify the reenroll trigger time, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
re-enroll-trigger-time percentage;
```

percentage is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

Specify the Regenerate Key Pair

When a regenerate key pair is configured, a new key pair is generated during reenrollment. On successful reenrollment, a new key pair and new certificate replace the old certificate and key pair. To generate a new key pair, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
re-generate-keypair;
```

Specify the Validity Period

The **validity-period** statement specifies the router certificate validity period, in number of days, that the specified router certificate remains valid. To specify the validity period, include the statement at the **[edit security pki auto-re-enrollment certificate-id certificate-name]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
  validity-period days;
```

days is the number of days for the validity period. The range can be from 1 through 4095.

Related Documentation

- [Digital Certificates Overview on page 174](#)
- [Configuring Digital Certificates for an ES PIC on page 177](#)

Configuring Auto-Reenrollment of a Router Certificate

Use the **auto-re-enrollment** statement to configure automatic reenrollment of a specified existing router certificate before its existing expiration date. This function automatically reenrolls the router certificate. The reenrollment process requests the certificate authority (CA) to issue a new router certificate with a new expiration date. The date of auto-reenrollment is determined by the following parameters:

- **re-enroll-trigger-time**—The percentage of the difference between the router certificate start date/time (when the certificate was generated) and the validity period; used to specify how long auto-reenrollment should be initiated before expiration.
- **validity-period**—The number of days after issuance when the router certificate will expire, as set when a certificate is generated.



NOTE: By default, this feature is not enabled unless configured explicitly. This means that a certificate that does not have auto-reenrollment configured will expire on its normal expiration date.

The **ca-profile** statement specifies which CA will be contacted to reenroll the expiring certificate. This is the CA that issued the original router certificate.

The **challenge-password** statement provides the issuing CA with the router certificate's password, as set by the administrator and normally obtained from the SCEP enrollment Web page of the CA. The password is 16 characters in length.

Optionally, the router certificate key pair can be regenerated by using the **re-generate-keypair** statement.

To configure automatic reenrollment properties, include the following statements at the **[edit security pki]** hierarchy level:

```
[edit security pki]
auto-re-enrollment {
  certificate-id {
    ca-profile ca-profile-name;
    challenge-password password;
    re-enroll-trigger-time-percentage percentage;
    re-generate-keypair;
    validity-period days;
  }
}
```

percentage is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

days is the number of days for the validity period. The range can be from 1 through 4095.

Tasks to configure automatic reenrollment of certificates are:

1. [Specify the Certificate ID on page 195](#)
2. [Specify the CA Profile on page 195](#)
3. [Specify the Challenge Password on page 196](#)
4. [Specify the Reenroll Trigger Time on page 196](#)
5. [Specify the Regenerate Key Pair on page 196](#)
6. [Specify the Validity Period on page 196](#)

Specify the Certificate ID

Use the **certificate-id** statement to specify the name of the router certificate to configure for auto-reenrollment. To specify the certificate ID, include the statement at the **[edit security pki auto-re-enrollment]** hierarchy level:

```
[edit security pki auto-re-enrollment]
certificate-id certificate-name;
```

Specify the CA Profile

Use the **ca-profile** statement to specify the name of the CA profile from the router certificate previously specified by certificate ID. To specify the CA profile, include the statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
ca-profile ca-profile-name;
```



NOTE: The referenced **ca-profile** must have an enrollment URL configured at the **[edit security pki ca-profile *ca-profile-name* enrollment url]** hierarchy level.

Specify the Challenge Password

The challenge password is used by the CA specified by the PKI certificate ID for reenrollment and revocation. To specify the challenge password, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
challenge-password password;
```

Specify the Reenroll Trigger Time

Use the **re-enroll-trigger-time** statement to set the percentage of the validity period before expiration at which reenrollment occurs. To specify the reenroll trigger time, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
re-enroll-trigger-time percentage;
```

percentage is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

Specify the Regenerate Key Pair

When a regenerate key pair is configured, a new key pair is generated during reenrollment. On successful reenrollment, a new key pair and new certificate replace the old certificate and key pair. To generate a new key pair, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
re-generate-keypair;
```

Specify the Validity Period

The **validity-period** statement specifies the router certificate validity period, in number of days, that the specified router certificate remains valid. To specify the validity period, include the statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
validity-period days;
```

days is the number of days for the validity period. The range can be from 1 through 4095.

IPsec Tunnel Traffic Configuration

- [IPsec Tunnel Traffic Configuration Overview on page 197](#)
- [Example: Configuring an Outbound Traffic Filter on page 199](#)

- [Example: Applying an Outbound Traffic Filter on page 199](#)
- [Example: Configuring an Inbound Traffic Filter for a Policy Check on page 200](#)
- [Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check on page 202](#)
- [ES Tunnel Interface Configuration for a Layer 3 VPN on page 203](#)

IPsec Tunnel Traffic Configuration Overview

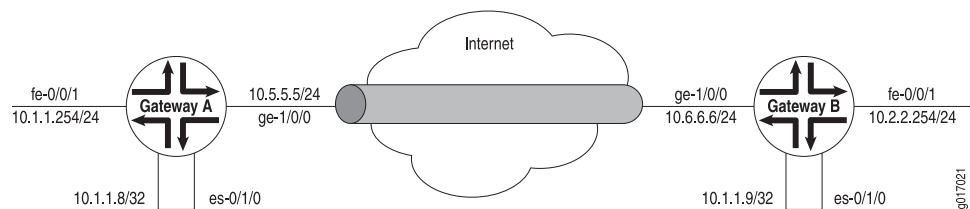
Traffic configuration defines the traffic that must flow through the IPsec tunnel. You configure outbound and inbound firewall filters, which identify and direct traffic to be encrypted and confirm that decrypted traffic parameters match those defined for the given tunnel. The outbound filter is applied to the LAN or WAN interface for the incoming traffic you want to encrypt off of that LAN or WAN. The inbound filter is applied to the ES PIC to check the policy for traffic coming in from the remote host. Because of the complexity of configuring a router to forward packets, no automatic checking is done to ensure that the configuration is correct. Make sure that you configure the router very carefully.



NOTE: The valid firewall filters statements for IPsec are **destination-port**, **source-port**, **protocol**, **destination-address**, and **source-address**.

In [Figure 11 on page 197](#), Gateway A protects the network 10.1.1.0/24, and Gateway B protects the network 10.2.2.0/24. The gateways are connected by an IPsec tunnel.

Figure 11: Example: IPsec Tunnel Connecting Security Gateways



The SA and ES interfaces for Gateway A are configured as follows:

```
[edit security ipsec]
security-association manual-sa1 {
  manual {
    direction bidirectional {
      protocol esp;
      spi 2312;
      authentication {
        algorithm hmac-md5-96;
        key ascii-text 1234123412341234;
      }
      encryption {
        algorithm 3des-cbc;
        key ascii-text 123456789009876543211234;
      }
    }
  }
}
```

```
    }  
  }  
}  
[edit interfaces es-0/1/0]  
unit 0 {  
  tunnel {  
    source 10.5.5.5;  
    destination 10.6.6.6;  
  }  
  family inet {  
    ipsec-sa manual-sa1;  
    address 10.1.1.8/32 {  
      destination 10.1.1.9;  
    }  
  }  
}
```

The SA and ES interfaces for Gateway B are configured as follows:

```
[edit security ipsec]  
security-association manual-sa1 {  
  manual {  
    direction bidirectional {  
      protocol esp;  
      spi 2312;  
      authentication {  
        algorithm hmac-md5-96;  
        key ascii-text 1234123412341234;  
      }  
      encryption {  
        algorithm 3des-cbc;  
        key ascii-text 123456789009876543211234;  
      }  
    }  
  }  
}  
[edit interfaces es-0/1/0]  
unit 0 {  
  tunnel {  
    source 10.6.6.6;  
    destination 10.5.5.5;  
  }  
  family inet {  
    ipsec-sa manual-sa1;  
    address 10.1.1.9/32 {  
      destination 10.1.1.8;  
    }  
  }  
}
```

- See Also**
- [Example: Configuring an Outbound Traffic Filter on page 199](#)
 - [Example: Applying an Outbound Traffic Filter on page 199](#)

- [Example: Configuring an Inbound Traffic Filter for a Policy Check on page 200](#)
- [ES Tunnel Interface Configuration for a Layer 3 VPN on page 203](#)

Example: Configuring an Outbound Traffic Filter

Firewall filters for outbound traffic direct the traffic through the desired IPsec tunnel and ensure that the tunneled traffic goes out the appropriate interface (see [“IPsec Tunnel Traffic Configuration Overview” on page 197](#)). Here, an outbound firewall filter is created on security Gateway A; it identifies the traffic to be encrypted and adds it to the input side of the interface that carries the internal VPN traffic:

```
[edit firewall]
filter ipsec-encrypt-policy-filter {
  term term1 {
    from {
      source-address { # local network
        10.1.1.0/24;
      }
      destination-address { # remote network
        10.2.2.0/24;
      }
    }
  }
  then ipsec-sa manual-sa1; # apply SA name to packet
  term default {
    then accept;
  }
}
```



NOTE: The source address, port, and protocol on the outbound traffic filter must match the destination address, port, and protocol on the inbound traffic filter. The destination address, port, and protocol on the outbound traffic filter must match the source address, port, and protocol on the inbound traffic filter.

- See Also**
- [Example: Applying an Outbound Traffic Filter on page 199](#)
 - [IPsec Tunnel Traffic Configuration Overview on page 197](#)

Example: Applying an Outbound Traffic Filter

After you have configured the outbound firewall filter, you apply it:

```
[edit interfaces]
fe-0/0/1 {
  unit 0 {
    family inet {
      filter {
        input ipsec-encrypt-policy-filter;
      }
    }
  }
}
```

```

        address 10.1.1.254/24;
    }
}

```

The outbound filter is applied on the Fast Ethernet interface at the **[edit interfaces fe-0/0/1 unit 0 family inet]** hierarchy level. Any packet matching the IPsec action term (**term 1**) on the input filter (**ipsec-encrypt-policy-filter**), configured on the Fast Ethernet interface, is directed to the ES PIC interface at the **[edit interfaces es-0/1/0 unit 0 family inet]** hierarchy level. If a packet arrives from the source address 10.1.1.0/24 and goes to the destination address 10.2.2.0/24, the Packet Forwarding Engine directs the packet to the ES PIC interface, which is configured with the **manual-sa1** SA. The ES PIC receives the packet, applies the **manual-sa1** SA, and sends the packet through the tunnel.

The router must have a route to the tunnel endpoint; add a static route if necessary.

See Also • [IPsec Tunnel Traffic Configuration Overview on page 197](#)

Example: Configuring an Inbound Traffic Filter for a Policy Check

- [Requirements on page 200](#)
- [Overview on page 200](#)
- [Configuration on page 200](#)

Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

Here, an inbound firewall filter, which performs the final IPsec policy check, is created on security Gateway A. This check ensures that only packets that match the traffic configured for this tunnel are accepted. This filter is configured via the CLI interface at the **[edit firewall family inet]** hierarchy level.

Configuration

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*.

To configure this example, perform the following tasks:

- [Configuring the firewall filter on page 201](#)

CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
[edit]
```

```

set firewall family inet filter ipsec-decrypt-policy-filter term term1 from source-address
  10.2.2.0/24
set firewall family inet filter ipsec-decrypt-policy-filter term term1 from destination-address
  10.1.1.0/24
set firewall family inet filter ipsec-decrypt-policy-filter term term1 then accept
commit

```

Configuring the firewall filter

Step-by-Step Procedure To configure the firewall filter, **ipsec-decrypt-policy-filter** that catches traffic from the remote 10.2.2.0/24 network that is destined for the local 10.1.1.0/24 network:

1. Create the firewall filter:

```

[edit]
user@host# edit firewall family inet filter ipsec-decrypt-policy-filter

```

2. Configure matching for source and destination addresses:

```

[edit firewall family inet filter ipsec-decrypt-policy-filter]
user@host# set term term1 from source-address 10.2.2.0/24
user@host# set term term1 from destination-address 10.1.1.0/24

```

3. Configure the filter to accept the matched traffic:

```

[edit firewall family inet filter ipsec-decrypt-policy-filter]
user@host# set term term1 then accept

```



NOTE: The accept statement within the term *term1* is for this filter only. Traffic that does not match this filter term will be dropped by the default firewall action.

4. Confirm your candidate firewall configuration by issuing the **show** configuration command at the **[edit firewall family inet]** hierarchy level

```

[edit firewall family inet]
user@host# show
filter ipsec-decrypt-policy-filter {
  term term1 { # perform policy check
    from {
      source-address { # remote network
        10.2.2.0/24;
      }
      destination-address { # local network
        10.1.1.0/24;
      }
    }
  }
}

```

```

    then accept;
  }
}

```

If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

5. If you are done configuring the device, commit your candidate configuration.

```

[edit]
user@host# commit

```

To implement this filter, you apply it as an input filter to the **es-0/1/0** logical interface of Gateway A. See [Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check](#) for details.

- See Also**
- [IPsec Tunnel Traffic Configuration Overview](#) on page 197
 - [Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check](#) on page 202

Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check

After you create the inbound firewall filter, apply it to the ES PIC. Here, the inbound firewall filter (**ipsec-decrypt-policy-filter**) is applied on the decrypted packet to perform the final policy check. The IPsec **manual-sa1** SA is referenced at the **[edit interfaces es-1/2/0 unit 0 family inet]** hierarchy level and decrypts the incoming packet.

```

[edit interfaces]
es-1/2/0 {
  unit 0 {
    tunnel {
      source 10.5.5.5; # tunnel source address
      destination 10.6.6.6; # tunnel destination address
    }
    family inet {
      filter {
        input ipsec-decrypt-policy-filter;
      }
      ipsec-sa manual-sa1; # SA name applied to packet
      address 10.1.1.8/32 { # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
    }
  }
}

```

The Packet Forwarding Engine directs IPsec packets to the ES PIC. It uses the packet's SPI, protocol, and destination address to look up the SA configured on one of the ES interfaces. The IPsec **manual-sa1** SA is referenced at the **[edit interfaces es-1/2/0 unit 0 family inet]** hierarchy level and is used to decrypt the incoming packet. When the packets

are processed (decrypted, authenticated, or both), the input firewall filter (**ipsec-decrypt-policy-filter**) is applied on the decrypted packet to perform the final policy check. Term1 defines the decrypted (and verified) traffic and performs the required policy check.



NOTE: The inbound traffic filter is applied after the ES PIC has processed the packet, so the decrypted traffic is defined as any traffic that the remote gateway is encrypting and sending to this router. IKE uses this filter to determine the policy required for a tunnel. This policy is used during the negotiation with the remote gateway to find the matching SA configuration.

See Also • [IPsec Tunnel Traffic Configuration Overview on page 197](#)

ES Tunnel Interface Configuration for a Layer 3 VPN

To configure an ES tunnel interface for a Layer 3 VPN, you need to configure an ES tunnel interface on the provider edge (PE) router and on the customer edge (CE) router. You also need to configure IPsec on the PE and CE routers.

See Also • [IPsec Tunnel Traffic Configuration Overview on page 197](#)

Tracing Operations for Security Services

- [Configuring Tracing Operations on page 203](#)
- [Configuring Tracing Operations for IPsec Events for Adaptive Services PICs on page 204](#)

Configuring Tracing Operations

To configure trace options for security services, specify flags using the **traceoptions** statement:

```
[edit security]
traceoptions {
  file filename <files number> <size size>;
  flag all;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
}
```

You can include these statements at the following hierarchy levels:

- **[edit security]**

- **[edit services ipsec-vpn]**

You can specify one or more of the following security tracing flags:

- **all**—Trace all security events
- **database**—Trace database events
- **general**—Trace general events
- **ike**—Trace IKE module processing
- **parse**—Trace configuration processing
- **policy-manager**—Trace policy manager processing
- **routing-socket**—Trace routing socket messages
- **timer**—Trace internal timer events

- See Also**
- [Configuring Tracing Operations for IPsec Events for Adaptive Services PICs on page 204](#)
 - *Security Associations Overview*

Configuring Tracing Operations for IPsec Events for Adaptive Services PICs

To configure trace options to trace IPsec events for Adaptive Services PICs, include the following statements at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
traceoptions {
  file filename <files number> <size size>;
  flag all;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
}
```

Trace option output is recorded in the `/var/log/kmd` file.

You can specify one or more of the following security tracing flags:

- **all**—Trace all security events
- **database**—Trace database events
- **general**—Trace general events
- **ike**—Trace IKE module processing
- **parse**—Trace configuration processing
- **policy-manager**—Trace policy manager processing

- **routing-socket**—Trace routing socket messages
- **timer**—Trace internal timer events

See Also • [Configuring Tracing Operations on page 203](#)

CHAPTER 10

Configuring SSH and SSL Router Access

- [Configuring SSH Host Keys for Secure Copying of Data on page 207](#)
- [Importing SSL Certificates for Junos XML Protocol Support on page 209](#)
- [Configuring IPsec for FIPS Mode on page 211](#)

Configuring SSH Host Keys for Secure Copying of Data

Secure Shell (SSH) uses encryption algorithms to generate a host, server, and session key system that ensures secure data transfer. You can configure SSH host keys to support secure copy (SCP) as an alternative to FTP for the background transfer of data such as configuration archives and event logs. To configure SSH support for SCP, you must complete the following tasks:

- Specify SSH known hosts by including hostnames and host key information in the Routing Engine configuration hierarchy.
- Set an SCP URL to specify the host from which to receive data. Setting this attribute automatically retrieves SSH host key information from the SCP server.
- Verify that the host key is authentic.
- Accept the secure connection. Accepting this connection automatically stores host key information in the local host key database. Storing host key information in the configuration hierarchy automates the secure handshake and allows background data transfer using SCP.

Tasks to configure SSH host keys for secure copying of data are:

1. [Configuring SSH Known Hosts on page 207](#)
2. [Configuring Support for SCP File Transfer on page 208](#)
3. [Updating SSH Host Key Information on page 209](#)

Configuring SSH Known Hosts

To configure SSH known hosts, include the **host** statement, and specify hostname and host key options for trusted servers at the **[edit security ssh-known-hosts]** hierarchy level:

```
[edit security ssh-known-hosts]
host corporate-archive-server, ip-address {
```

```

    dsa-key key;
  }
  host archive-server-url {
    rsa-key key;
  }
  host server-with-ssh-version-1, ip-address {
    rsa1-key key;
  }

```

Host keys are one of the following:

- **dsa-key key**—Base64 encoded Digital Signature Algorithm (DSA) key for SSH version 2.
- **ecdsa-sha2-nistp256-key key**—Base64 encoded ECDSA-SHA2-NIST256 key.
- **ecdsa-sha2-nistp384-key key**—Base64 encoded ECDSA-SHA2-NIST384 key.
- **ecdsa-sha2-nistp521-key key**—Base64 encoded ECDSA-SHA2-NIST521 key.
- **ed25519-key key**—Base64 encoded ED25519 key.
- **rsa-key key**—Base64 encoded public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.
- **rsa1-key key**—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.

Starting in Junos OS Release 18.3R1, the **ssh-dss** and **ssh-dsa** hostkey algorithms are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Configuring Support for SCP File Transfer

To configure a known host to support background SCP file transfers, include the **archive-sites** statement at the **[edit system archival configuration]** hierarchy level.

```

[edit system archival configuration]
archive-sites {
  scp://username<:password>@host<:port>/url-path;
}

```



NOTE: When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (") and enclose the IPv6 host address in brackets ([]). For example, "scp://username<:password>@[host]<:port>/url-path";

Setting the **archive-sites** statement to point to an SCP URL triggers automatic host key retrieval. At this point, Junos OS connects to the SCP host to fetch the SSH public key, displays the host key message digest or fingerprint as output to the console, and terminates the connection to the server.

```
user@host# set system archival configuration archive-sites "<scp-url-path>"
The authenticity of host <my-archive-server (<server-ip-address>)> can't be established.
RSA key fingerprint is <ascii-text key>. Are you sure you want to continue connecting
(yes/no)?
```

To verify that the host key is authentic, compare this fingerprint with a fingerprint that you obtain from the same host using a trusted source. If the fingerprints are identical, accept the host key by entering **yes** at the prompt. The host key information is then stored in the Routing Engine configuration and supports background data transfers using SCP.

Updating SSH Host Key Information

Typically, SSH host key information is automatically retrieved when you set a URL attribute for SCP using the **archival configuration archive-sites** statement at the **[edit system]** hierarchy level. However, if you need to manually update the host key database, use one of the following methods.

1. [Retrieving Host Key Information Manually on page 209](#)
2. [Importing Host Key Information from a File on page 209](#)

Retrieving Host Key Information Manually

To manually retrieve SSH public host key information, use the **fetch-from-server** option with the **set security ssh-known-hosts** command. You must include a hostname attribute with the **set security ssh-known-hosts fetch-from-server** command to specify the host from which to retrieve the SSH public key.

```
user@host# set security ssh-known-hosts fetch-from-server <hostname>
```

Importing Host Key Information from a File

To manually import SSH host key information from the known-hosts file located at **/var/tmp/known-hosts** on the server, include the **load-key-file** option with the **set security ssh-known-hosts** command. You must include the path to the **known-hosts** file with the **set security ssh-known-hosts load-key-file** command to specify the location from which to import host key information.

```
user@host# set security ssh-known-hosts load-key-file /var/tmp/known-hosts
```

See Also • [Importing SSL Certificates for Junos XML Protocol Support on page 209](#)

Importing SSL Certificates for Junos XML Protocol Support



NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.

A Junos XML protocol client application can use one of four protocols to connect to the Junos XML protocol server on a router or switch: clear-text (a Junos XML protocol-specific protocol for sending unencrypted text over a TCP connection), SSH, SSL, or Telnet. For clients to use the SSL protocol, you must copy an X.509 authentication certificate onto the router or switch, as described in this topic. You must also include the **xnm-ssl** statement at the **[edit system services]** hierarchy level.



NOTE: The **xnm-ssl** statement does not apply to standard IPsec services.

After obtaining an X.509 authentication certificate and private key, copy it to the router or switch by including the **local** statement at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
local certificate-name {
  load-key-file (filename | url);
}
```

certificate-name is a name you choose to identify the certificate uniquely (for example, **Junos XML protocol-ssl-client-hostname**, where **hostname** is the computer where the client application runs).

filename is the pathname of the file on the local disk that contains the paired certificate and private key (assuming you have already used another method to copy them to the router's or switch's local disk).

url is the URL to the file that contains a paired certificate and private key (for instance, on the computer where the Junos XML protocol client application runs).



NOTE: The CLI expects the private key in the **URL-or-path** file to be unencrypted. If the key is encrypted, the CLI prompts you for the passphrase associated with it, decrypts it, and stores the unencrypted version.

The **load-key-file** statement acts as a directive that copies the contents of the certificate file into the configuration. When you view the configuration, the CLI displays the string of characters that constitute the private key and certificate, marking them as **SECRET-DATA**. The **load-key-file** keyword is not recorded in the configuration.

**Related
Documentation**

- *Configuring SSH Host Keys for Secure Copying of Data*
- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*

Configuring IPsec for FIPS Mode

- [Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 211](#)
- [Example: Configuring Internal IPsec on page 214](#)

Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode

In a Junos OS in FIPS mode environment, routers with two Routing Engines must use IPsec for internal communication between the Routing Engines. You configure internal IPsec after you install the Junos OS in FIPS mode. You must be a Crypto Officer to configure internal IPsec.



NOTE: You cannot configure DES-based IPsec SAs in Junos OS in FIPS mode. The internal IPsec SAs use HMAC-SHA1-96 authentication and 3DES-CBC encryption.

Manual SAs require no negotiation. All values, including the keys, are static and specified in the configuration. Manual SAs statically define the SPI values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.



NOTE: When the switch is in FIPS mode, you cannot use the `commit synchronize` command until you have established an IPsec SA on each Routing Engine.

As Crypto Officer, you configure an internal IPsec SA for communication between Routing Engines by creating an SA on each Routing Engine with the following statements at the `[security]` hierarchy level:

To configure internal IPsec, include the `security-association` statement at the `[security]` hierarchy level. You can configure parameters, such as the direction in which the manual IPsec SAs must be applied, the SPI value that uniquely identifies the SA to use at the receiving Routing Engine, and the IPsec key that defines the authentication and encryption keys for the manual IPsec SA.

```
[ security]
ipsec {
  internal {
    security-association {
      manual {
        direction (bidirectional | inbound | outbound) {
          protocol esp;
          spi spi-value;
          encryption {
            algorithm (hmac-sha1-96 | hmac-sha2-256);
```

```

    key (ascii-text ascii-text-string | hexadecimal hexadecimal-number);
  }
}
}
}
}

```

Tasks for configuring internal IPsec for Junos-FIPS are the following. You can configure the direction in which the manual IPsec SAs must be applied, the SPI value that uniquely identifies the SA to use at the receiving Routing Engine, and the IPsec key that defines the authentication and encryption keys for the manual IPsec SA.

1. [Configuring the SA Direction on page 212](#)
2. [Configuring the IPsec SPI on page 213](#)
3. [Configuring the IPsec Key on page 213](#)

Configuring the SA Direction

To configure the IPsec SA direction in which manual SAs of the IPsec tunnels must be applied, include the **direction** statement at the **[security ipsec internal security-association manual]** hierarchy level:

```
direction (bidirectional | inbound | outbound);
```

The value can be one of the following:

- **bidirectional**—Apply the same SA values in both directions between Routing Engines.
- **inbound**—Apply these SA properties only to the inbound IPsec tunnel.
- **outbound**—Apply these SA properties only to the outbound IPsec tunnel.

If you do not configure the SA to be bidirectional, you must configure SA parameters for IPsec tunnels in both the inbound and outbound directions. The following example uses an inbound and outbound IPsec tunnel:



NOTE: We recommend that you do not use the IPsec keys as ASCII keys for Junos OS in FIPS mode. Instead, you must use the IPsec keys as hexadecimal keys for maximum key strength.

```

[security]
ipsec {
  internal {
    security-association {
      manual {
        direction inbound {
          protocol esp;
          spi 512;
          encryption {

```



```

        algorithm 3des-cbc;
        key hexadecimal 309fc4be20f04e53e011b00744642d3fe66c2c7c;
    }
}
direction outbound {
    protocol esp;
    spi 513;
    encryption {
        algorithm 3des-cbc;
        key hexadecimal b0344c61d8db38535ca8afceaf0bf12b881dc200c9833da7;
    }
}
}
}
}
}
}

```

Configuring the IPsec SPI

A security parameter index (SPI) is a 32-bit index that identifies a security context between a pair of Routing Engines. To configure the IPsec SPI value, include the **spi** statement at the **[security ipsec internal security-association manual direction]** hierarchy level:

```
spi value;
```

The value must be from 256 through 16,639.

Configuring the IPsec Key



NOTE: We recommend that you do not use the IPsec keys as ASCII keys for Junos OS in FIPS mode. Instead, you must use the IPsec keys as hexadecimal keys for maximum key strength.

The distribution and management of keys are critical to using VPNs successfully. You must configure the ASCII text key values for authentication and encryption. To configure the ASCII text key, include the **key** statement at the **[security ipsec internal security-association manual direction encryption]** hierarchy level:

```
key (ascii-text ascii-text-string | hexadecimal hexadecimal-string);
```

For this type of SA, both keys must be preshared hexadecimal values, and each requires a specific cryptographic algorithm:

- Authentication algorithm
 - HMAC-SHA1-96 (40 characters)
 - HMAC-SHA2-256 (64 characters)
- Encryption algorithm

- 3DES-CBC (48 characters)

You must enter the key hexadecimal value twice and the strings entered must match, or the key will not be set. The hexadecimal key is never displayed in plain text. We recommend that you use the IPsec keys as hexadecimal keys for maximum key strength and not as ASCII keys for Junos OS in FIPS mode.

See Also • [Example: Configuring Internal IPsec on page 214](#)

Example: Configuring Internal IPsec

Configure a bidirectional IPsec SA with an SPI value of 512 and a key value conforming to the FIPS 140-2 rules:

```
[edit security]
ipsec {
  internal {
    security-association {
      manual {
        direction bidirectional {
          protocol esp;
          spi 512;
          encryption {
            algorithm 3des-cbc;
            key ascii-text "$ABC123";
          }
        }
      }
    }
  }
}
```

See Also • [Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 211](#)

PART 4

MACsec

- [Understanding MACsec on page 217](#)
- [MACsec Examples on page 249](#)

CHAPTER 11

Understanding MACsec

- [Understanding Media Access Control Security \(MACsec\) on page 217](#)

Understanding Media Access Control Security (MACsec)

- [Understanding Media Access Control Security \(MACsec\) on page 217](#)
- [Configuring MACsec on EX, SRX and Fusion Devices on page 228](#)

Understanding Media Access Control Security (MACsec)

Media Access Control Security (MACsec) is an 802.1AE IEEE industry-standard security technology that provides secure communication for all traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks.

MACsec allows you to secure an Ethernet link for almost all traffic, including frames from the Link Layer Discovery Protocol (LLDP), Link Aggregation Control Protocol (LACP), Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), and other protocols that are not typically secured on an Ethernet link because of limitations with other security solutions. MACsec can be used in combination with other security protocols such as IP Security (IPsec) and Secure Sockets Layer (SSL) to provide end-to-end network security.

MACsec is standardized in IEEE 802.1AE. The IEEE 802.1AE standard can be seen on the IEEE organization website at [IEEE 802.1: BRIDGING & MANAGEMENT](#).

Starting in Junos OS Release 18.2R1, MACsec is supported on ACX6360 routers.

Starting with Junos OS Release 15.1 for MX Series routers, MACsec enables you to secure an Ethernet link for almost all traffic, including frames from the Link Layer Discovery Protocol (LLDP), Link Aggregation Control Protocol (LACP), Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), and other protocols that are not typically secured on an Ethernet link because of limitations with other security solutions.

- [How MACsec Works on page 218](#)
- [Understanding Connectivity Associations and Secure Channels on page 219](#)
- [Understanding Static Connectivity Association Key Security Mode \(Security Mode for Router-to-Router Links\) on page 219](#)

- [Understanding MACsec Hardware Requirements for MX and PTX Series Routers on page 220](#)
- [Understanding MACsec Software Requirements for MX Series Routers on page 220](#)
- [Understanding MACsec Security Modes for Switch-to-Switch Links on page 221](#)
- [Understanding the Requirements to Enable MACsec on a Switch-to-Host Link on page 223](#)
- [MACsec Software Image Requirements for EX Series and QFX Series Switches on page 224](#)
- [MACsec Hardware and Software Support Summary on page 225](#)
- [Understanding MACsec in a Virtual Chassis on page 227](#)
- [Understanding the MACsec Feature License Requirement on page 227](#)
- [MACsec Limitations on page 228](#)

How MACsec Works

MACsec provides industry-standard security through the use of secured point-to-point Ethernet links. The point-to-point links are secured after matching security keys are exchanged and verified between the interfaces at each end of the point-to-point Ethernet link. The key can be user-configured or can be generated dynamically, depending on the security mode used to enable MACsec. For more information on MACsec security modes, see [“Understanding MACsec Security Modes for Switch-to-Switch Links” on page 221](#). Other user-configurable parameters, such as MAC address or port, must also match on the interfaces on each side of the link to enable MACsec.



NOTE: On MX Series routers, you enable MACsec by using the static CAK security mode. See [“Configuring MACsec on EX, SRX and Fusion Devices” on page 228](#).

Once MACsec is enabled on a point-to-point Ethernet link, all traffic traversing the link is MACsec-secured through the use of data integrity checks and, if configured, encryption.

The data integrity checks verify the integrity of the data. MACsec appends an 8-byte header and a 16-byte tail to all Ethernet frames traversing the MACsec-secured point-to-point Ethernet link, and the header and tail are checked by the receiving interface to ensure that the data was not compromised while traversing the link. If the data integrity check detects anything irregular about the traffic, the traffic is dropped.

MACsec can also be used to encrypt all traffic on the Ethernet link. The encryption used by MACsec ensures that the data in the Ethernet frame cannot be viewed by anybody monitoring traffic on the link. MACsec encryption is optional and user-configurable; you can enable MACsec to ensure the data integrity checks are performed while still sending unencrypted data “in the clear” over the MACsec-secured link, if desired.

MACsec is configured on point-to-point Ethernet links between MACsec-capable interfaces. If you want to enable MACsec on multiple Ethernet links, you must configure MACsec individually on each point-to-point Ethernet link.

On MX Series routers, you can configure the **set security macsec connectivity-association connectivity-association-name exclude-protocol** command to specify protocols whose packets are not secured using Media Access Control Security (MACsec) when MACsec is enabled on a link by using static connectivity association key (CAK) security mode. When this option is enabled in a connectivity association that is attached to an interface, MACsec is not enabled for all packets of the specified protocols that are sent and received on the link.

Understanding Connectivity Associations and Secure Channels

MACsec is configured in connectivity associations. MACsec is enabled when a connectivity association is assigned to an interface.

When you are configuring MACsec using static secure association key (SAK) security mode, you must configure secure channels within a connectivity association. The secure channels are responsible for transmitting and receiving data on the MACsec-enabled link, and also responsible for transmitting SAKs across the link to enable and maintain MACsec. A single secure channel is unidirectional— it can be used to apply MACsec only to either inbound or outbound traffic. A typical connectivity association when MACsec is enabled using SAK security mode contains two secure channels— one secure channel for inbound traffic and another secure channel for outbound traffic.

When you enable MACsec using static CAK or dynamic security mode, you have to create and configure a connectivity association. Two secure channels— one secure channel for inbound traffic and another secure channel for outbound traffic— are automatically created. The automatically-created secure channels do not have any user-configurable parameters; all configuration is done in the connectivity association outside of the secure channels.

Understanding Static Connectivity Association Key Security Mode (Security Mode for Router-to-Router Links)

When you enable MACsec using static connectivity association key (CAK) security mode, two security keys—a connectivity association key (CAK) that secures control plane traffic and a randomly-generated secure association key (SAK) that secures data plane traffic—are used to secure the point-to-point Ethernet link.

You initially establish a MACsec-secured link using a preshared key when you are using static CAK security mode to enable MACsec. A preshared key includes a connectivity association name (CKN) and a connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

The preshared keys must be configured on the endpoints of the link and the keys must be in agreement with each other. The MACsec Key Agreement (MKA) protocol is responsible for maintaining MACsec on the link, and decides which router on the point-to-point link becomes the key server. The key server then creates an SAK that is shared with the router at the other end of the point-to-point link only, and that SAK is used to secure all data traffic traversing the link. The key server continues to periodically create and share a randomly-created SAK over the point-to-point link for as long as MACsec is enabled.

See “Configuring Media Access Control Security (MACsec) on MX Series Routers” on page 268 for step-by-step instructions on enabling MACsec by using static CAK security mode.

Understanding MACsec Hardware Requirements for MX and PTX Series Routers

Table 8 on page 220 lists the line cards which support MACsec.

Table 8: Line cards and MICs supporting MACsec on MX series and PTX series Routers

Line Card	Router	Version
MIC-3D-20GE-SFP-E	MX240, MX480, and MX960	14.2 and 15.1
MPC7E-10G	MX240, MX480, MX960, MX2010, and MX2020	16.1
JNP-MIC1-MACSEC	MX10003	17.3R2
PTX10K-LC1105	PTX10008	18.2R1
PTX10K-LC1105	PTX10008 and PTX10016	18.3R1
MPC10E-15C and MPC10E-10C	MX240, MX480, MX960, MX2010, and MX2020	19.1R1

MACsec can also be configured on supported MX Series router interfaces when those routers are configured in a Virtual Chassis configuration. Encryption and decryption are implemented in the hardware in line-rate mode. An additional overhead of 24 through 32 bytes is required for MACsec if Secure Channel Identifier (SCI) tag is included.

For more information regarding MACsec, refer the following IEEE specifications:

- IEEE 802.1AE-2006. Media Access Control (MAC) Security
- IEEE 802.1X-2010. Port-Based Network Access Control. Defines MACSec Key Agreement Protocol

Understanding MACsec Software Requirements for MX Series Routers

Following are some of the key software requirements for MACsec on MX Series Routers:



NOTE: A feature license is not required to configure MACsec on MX Series routers with the enhanced 20-port Gigabit Ethernet MIC (model number MIC-3D-20GE-SFP-E).

MACsec is supported on MX Series routers with MACsec-capable interfaces.

MACsec supports 128 and 256-bit cipher-suite with and without extended packet numbering (XPN).

MACsec supports MACsec Key Agreement (MKA) protocol with Static-CAK mode using preshared keys.

MACsec supports a single connectivity-association (CA) per physical port or physical interface.

Starting with Junos OS Release 15.1, MACsec is supported on member links of an aggregated Ethernet (**ae-**) interface bundle, and also regular interfaces that are not part of an interface bundle.

Starting with Junos OS Release 17.3R2, MACsec supports 256-bit cipher-suite GCM-AES-256 and GCM-AES-XPB-256 on MX10003 routers with the modular MIC (model number-JNP-MIC1-MACSEC).

Starting in Junos OS Release 18.4R2, the MIC-MACSEC-20GE MIC provides 256-bit cipher-suite GCM-AES-256 and GCM-AES-XPB-256. The MIC-MACSEC-20GE MIC supports MACsec on both twenty 1-Gigabit Ethernet SFP ports and on two 10-Gigabit Ethernet SFP+ ports in the following hardware configurations:

- Installed directly on the MX80 and MX104 routers
- Installed on MPC1, MPC2, MPC3, MPC2E, MPC3E, MPC2E-NG, and MPC3E-NG line cards on the MX240, MX480, and MX960 routers

Refer *Understanding Interface Naming Conventions for MIC-MACSEC-20GE* and *Understanding Rate Selectability* for more information.

Understanding MACsec Security Modes for Switch-to-Switch Links

Understanding Static Connectivity Association Key Security Mode

When you enable MACsec using static connectivity association key (CAK) security mode, two security keys— a connectivity association key (CAK) that secures control plane traffic and a randomly-generated secure association key (SAK) that secures data plane traffic—are used to secure the point-to-point Ethernet link. Both keys are regularly exchanged between both devices on each end of the point-to-point Ethernet link to ensure link security.

You initially establish a MACsec-secured link using a pre-shared key when you are using static CAK security mode to enable MACsec. A pre-shared key includes a connectivity association name (CKN) and its own connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

Once matching pre-shared keys are successfully exchanged, the MACsec Key Agreement (MKA) protocol is enabled. The MKA protocol is responsible for maintaining MACsec on the link, and decides which switch on the point-to-point link becomes the key server. The key server then creates an SAK that is shared with the switch at the other end of the point-to-point link only, and that SAK is used to secure all data traffic traversing the link. The key server will continue to periodically create and share a randomly-created SAK over the point-to-point link for as long as MACsec is enabled.



NOTE: If the MACsec session is terminated due to a link failure, when the link is restored, the MKA key server elects a key server and generates a new SAK.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels— one for inbound traffic and one for outbound traffic— are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

We recommend enabling MACsec on switch-to-switch links using static CAK security mode. Static CAK security mode ensures security by frequently refreshing to a new random security key and by sharing only the security key between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features— replay protection, SCI tagging, and the ability to exclude traffic from MACsec— are available only when you enable MACsec using static CAK security mode.



NOTE: The switches on each end of a MACsec-secured switch-to-switch link must either both be using Junos OS Release 14.1X53-D10 or later, or must both be using an earlier version of Junos, in order to establish a MACsec-secured connection when using static CAK security mode.

See [“Configuring MACsec on EX, SRX and Fusion Devices” on page 228](#) for step-by-step instructions on enabling MACsec using static CAK security mode.

Understanding Dynamic Secure Association Key Security Mode (Switch-to-Host Links)

Dynamic secure association key (SAK) security mode is used to enable MACsec on a switch-to-host link.

To enable MACsec on a link connecting an endpoint device—such as a server, phone, or personal computer—to a switch, the endpoint device must support MACsec and must be running software that allows it to enable a MACsec-secured connection. When configuring MACsec on a switch-to-host link, the MACsec Key Agreement (MKA) keys, which are included as part of 802.1X authentication, are retrieved from a RADIUS server as part of the AAA handshake. A master key is passed from the RADIUS server to the switch and from the RADIUS server to the host in independent authentication transactions. The master key is then passed between the switch and the host to create a MACsec-secured connection.

A secure association using dynamic secure association security mode must be configured on the switch’s Ethernet interface that connects to the host in order for the switch to create a MACsec-secured connection after receiving the MKA keys from the RADIUS server.

The RADIUS server must be using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) in order to support MACsec. The RADIUS servers that support other widely-used authentication frameworks, such as password-only or md5, cannot be used to support MACsec. In order to enable MACsec on a switch to secure a connection to a host, you must be using 802.1X authentication on the RADIUS server. MACsec must be configured into dynamic mode. MACsec is still enabled using connectivity associations when enabled on a switch-to-host link, as it is on a switch-to-switch link.

Understanding Static Secure Association Key Security Mode (Supported for Switch-to-Switch Links)

When you enable MACsec using static secure association key (SAK) security mode, one of up to two manually configured SAKs is used to secure data traffic on the point-to-point Ethernet link. All SAK names and values are configured by the user; there is no key server or other tool that creates SAKs. Security is maintained on the point-to-point Ethernet link by periodically rotating between the two security keys. Each security key name and value must have a corresponding matching value on the interface at the other end of the point-to-point Ethernet link to maintain MACsec on the link.

You configure SAKs within secure channels when you enable MACsec using static SAK security mode. You configure secure channels within connectivity associations. A typical connectivity association for MACsec using static SAK security mode contains two secure channels— one for inbound traffic and one for outbound traffic— that have each been configured with two manually-configured SAKs. You must attach the connectivity association with the secure channel configurations to an interface to enable MACsec using static SAK security mode.

We recommend enabling MACsec using static CAK security mode. Use static SAK security mode only if you have a compelling reason to use it instead of static CAK security mode.

See [“Configuring MACsec on EX, SRX and Fusion Devices” on page 228](#) for step-by-step instructions on enabling MACsec using SAKs.

Understanding the Requirements to Enable MACsec on a Switch-to-Host Link

When configuring MACsec on a switch-to-host link, the MACsec Key Agreement (MKA) keys, which are included as part of 802.1X authentication, are retrieved from a RADIUS server as part of the AAA handshake. A master key is passed from the RADIUS server to the switch and from the RADIUS server to the host in independent authentication transactions. The master key is then passed between the switch and the host to create a MACsec-secured connection.

The following requirements must be met in order to enable MACsec on a link connecting a host device to a switch.

The host device:

- must support MACsec and must be running software that allows it to enable a MACsec-secured connection with the switch.

The switch:

- must support MACsec (see [Table 9 on page 225](#)).
- must be configured into dynamic secure association key security mode.
- must be using 802.1X authentication to communicate with the RADIUS server.

The RADIUS server:

- must be using the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework.



NOTE: RADIUS servers that support other widely-used authentication frameworks, such as password-only or md5, cannot be used to support MACsec.

- must be using 802.1X authentication.
- can be multiple hops from the switch and the host device.

MACsec Software Image Requirements for EX Series and QFX Series Switches

Junos OS Release 16.1 and Later

For Junos OS Release 16.1 and later, you must download the standard Junos image to enable MACsec. MACsec is not supported in the limited image. See the [“MACsec Hardware and Software Support Summary” on page 225](#) to determine the correct release for your device.

The standard version of Junos OS software contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of this Junos OS software is strictly controlled under United States export laws. The export, import, and use of this Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring this version of your Junos OS software, contact Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

Junos OS Releases Prior to 16.1

For releases prior to Junos OS Release 16.1, you must download the controlled version of your Junos OS software to enable MACsec. MACsec support is not available in the domestic version of Junos OS software in releases prior to Junos OS Release 16.1. See the [“MACsec Hardware and Software Support Summary” on page 225](#) to determine the correct release for your device.

The controlled version of Junos OS software includes all features and functionality available in the domestic version of Junos OS, while also supporting MACsec. The domestic version of Junos OS software is shipped on all switches that support MACsec, so you must download and install a controlled version of Junos OS software for your switch before you can enable MACsec.

The controlled version of Junos OS software contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS software is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring the controlled version of your Junos OS software, contact Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

MACsec Hardware and Software Support Summary

Table 9 on page 225 summarizes MACsec hardware and software support for EX Series and QFX Series switches.

See [Feature Explorer](#) for a full listing of Junos OS releases and platforms that support MACsec.

Table 9: MACsec Hardware and Software Support Summary for EX Series and QFX Series Switches

Switch	MACsec-capable Interfaces	Switch-to-Switch Support Introduction	Switch-to-Host Support Introduction	Encryption
EX3400	10GbE fiber interfaces and 1GbE copper interfaces.	15.1X53-D50	15.1X53-D50	AES-128 <i>NOTE:</i> MACsec is not available on the limited Junos OS image package.
EX4200	All uplink port connections on the SFP+ MACsec uplink module.	13.2X50-D15	14.1X53-D10	AES-128
EX4300	All access and uplink ports. Both QSFP+ interfaces on the EX-UM-2QSFP-MR uplink module for EX4300-48MP switches.	13.2X50-D15	14.1X53-D10	AES-128 AES-256 (EX4300-48MP only)
EX4550	All EX4550 optical interfaces that use the LC connection type. See <i>Pluggable Transceivers Supported on EX4550 Switches</i> .	13.2X50-D15	14.1X53-D10	AES-128
EX4600	All twenty-four fixed 1GbE SFP/10GbE SFP+ interfaces and all interfaces that support the copper Gigabit Interface Converter (GBIC). All eight SFP+ interfaces on the EX4600-EM-8F expansion module.	14.1X53-D15 <i>NOTE:</i> MACsec is not supported on EX4600 in Junos OS Release 15.1.	Not supported	AES-128

Table 9: MACsec Hardware and Software Support Summary for EX Series and QFX Series Switches (continued)

Switch	MACsec-capable Interfaces	Switch-to-Switch Support Introduction	Switch-to-Host Support Introduction	Encryption
EX9200	<p>All forty SFP interfaces on the EX9200-40F-M line card.</p> <p>All twenty SFP interfaces on the EX9200-20F-MIC installed in an EX9200-MPC line card.</p> <p>NOTE: You can install up to two EX9200-20F-MIC MICs in an EX9200-MPC line card for a maximum of forty MACsec-capable interfaces.</p> <p>All forty SFP+ interfaces on the EX9200-40XS.</p>	15.1R1	15.1R1	<p>AES-128</p> <p>NOTE: Starting in Junos OS Release 18.2R1, AES-256 is supported on the EX9200-40XS line card.</p>
QFX5100	All eight SFP+ interfaces on the EX4600-EM-8F expansion module installed in a QFX5100-24Q switch.	<p>14.1X53-D15</p> <p>NOTE: MACsec is not supported on QFX5100-24Q switches in Junos OS Release 15.1.</p>	Not supported	AES-128

Table 9: MACsec Hardware and Software Support Summary for EX Series and QFX Series Switches (continued)

Switch	MACsec-capable Interfaces	Switch-to-Switch Support Introduction	Switch-to-Host Support Introduction	Encryption
QFX10008 and QFX10016	All six interfaces on the QFX10000-6C-DWDM line card.	17.2R1 NOTE: Static CAK mode only.	Not supported	AES-128 and AES-256 NOTE: When enabling MACsec on the QFX10000-6C-DWDM line card, we recommend using a cipher suite with extended packet numbering (XPN). Supported XPN cipher suites are GCM-AES-XPN-128 and GCM-AES-XPN-256.
	All 30 interfaces on the QFX10000-30C-M line card.	17.4R1 NOTE: Static CAK mode only.	Not supported	AES-128 and AES-256 NOTE: When enabling MACsec on the QFX10000-30C-M line card, we recommend using a cipher suite with extended packet numbering (XPN). Supported XPN cipher suites are GCM-AES-XPN-128 and GCM-AES-XPN-256.

Understanding MACsec in a Virtual Chassis

MACsec can be configured on supported switch interfaces when those switches are configured in a Virtual Chassis or Virtual Chassis Fabric (VCF), including when MACsec-supported interfaces are on member switches in a mixed Virtual Chassis or VCF that includes switch interfaces that do not support MACsec. MACsec, however, cannot be enabled on Virtual Chassis ports (VCPs) to secure traffic travelling between member switches in a Virtual Chassis or VCF.

Understanding the MACsec Feature License Requirement

A feature license is required to configure MACsec on EX Series and QFX series switches, with the exception of the QFX10000-6C-DWDM and QFX10000-30C-M line cards. If the MACsec licence is not installed, MACsec functionality cannot be activated.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (<https://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key. You will

be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

The MACsec feature license is an independent feature license; the feature licenses that must be purchased to enable other groups of features on your switches cannot be purchased to enable MACsec. Two MACsec license are required per Virtual Chassis Fabric (VCF) and per Virtual Chassis (VC).

MACsec Limitations

- All types of Spanning Tree Protocol frames cannot currently be encrypted using MACsec.
- MACsec traffic drops are expected during GRES switchover.
- On EX4300 switches, MACsec might not work properly on PHY84756 1G SFP ports if auto negotiation is enabled and MACsec is configured on those ports. As a workaround, configure **no- auto-negotiation** on PHY84756 1G SFP ports before configuring MACsec on those ports.

- See Also**
- [Configuring MACsec on EX, SRX and Fusion Devices on page 228](#)
 - [cipher-suite on page 704](#)

Configuring MACsec on EX, SRX and Fusion Devices

Media Access Control Security (MACsec) is an industry-standard security technology that provides secure communication for almost all types of traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly-connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec is standardized in IEEE 802.1AE.

You can configure MACsec to secure point-to-point Ethernet links connecting EX Series or QFX Series switches, or on Ethernet links connecting a switch to a host device such as a PC, phone, or server. Each point-to-point Ethernet link that you want to secure using MACsec must be configured independently. You can enable MACsec on switch-to-switch links using static secure association key (SAK) security mode or static connectivity association key (CAK) security mode. Both processes are provided in this document.



BEST PRACTICE: We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

The configuration steps for both processes are provided in this document.



BEST PRACTICE: When enabling MACsec, we recommend that when you examine your interface MTU, adjusting it for MACsec overhead, which is 32 bytes.



NOTE: This topic pertains to switches that support MACsec. Any specifics about a particular switch are identified as such.

- [Acquiring and Downloading the Junos OS Software on page 229](#)
- [Acquiring and Downloading the MACsec Feature License on page 230](#)
- [Configuring the PIC Mode of the MACsec-capable Interfaces \(EX4200 switches only\) on page 231](#)
- [Configuring MACsec Using Static Connectivity Association Key Security Mode \(Recommended for Enabling MACsec on Switch-to-Switch Links\) on page 233](#)
- [Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link on page 238](#)
- [Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link on page 243](#)

Acquiring and Downloading the Junos OS Software

For Junos OS Release 16.1 and later, you must download the standard Junos image to enable MACsec. MACsec is not supported in the limited image.

For releases prior to Junos OS Release 16.1, you must download the controlled version of your Junos OS software to enable MACsec. MACsec support is not available in the domestic version of Junos OS software in releases prior to Junos OS Release 15.1.

You can identify whether a software package is the standard or controlled version of Junos OS by viewing the package name. A software package for a controlled version of Junos OS is named using the following format:

```
package-name-m.nZx.y-controlled-signed.tgz
```

A software package for a standard version of Junos OS is named using the following format:

```
package-name-m.nZx.y-.tgz
```

If you are unsure which version of Junos OS is running on your switch, enter the **show version** command. If the **JUNOS Crypto Software Suite** description appears in the output, you are running the controlled version of Junos OS. If you are running a controlled version of Junos OS, enter the **show system software** command to display the version. The output also shows the version of all loaded software packages.

The controlled version of Junos OS software for EX Series or QFX Series switches contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS software is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring the controlled version of your Junos OS software, contact Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

The standard version of Junos OS software for EX Series and QFX Series switches contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of this Junos OS software is strictly controlled under United States export laws. The export, import, and use of this Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring this version of your Junos OS software, contact Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

The process for installing the controlled or standard version of Junos OS software onto your switch is identical to installing any other version of Junos OS software. You must enter the **request system software add** statement to download the Junos OS image, and the **request system reboot** statement to reboot the switch to complete the upgrade procedure.

See “[Understanding Media Access Control Security \(MACsec\)](#)” on page 217 for additional information on the versions of Junos OS software that are required for MACsec.

[Acquiring and Downloading the MACsec Feature License](#)

A feature license is required to configure MACsec on an EX Series or a QFX Series switch, with the exception of the QFX10000-6C-DWDM and QFX10000-30C-M line cards. If the MACsec licence is not installed, MACsec functionality cannot be activated.

The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series or QFX Series switches cannot be purchased to enable MACsec.

To purchase a software license for MACsec, contact your Juniper Networks sales representative (<https://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key. You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

For a Virtual Chassis deployment, two MACsec license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role

To add one or more new MACsec license keys on the switch, follow this procedure:

1. Add the license key or keys:
 - To add one or more license keys from a file or URL, specify the filename of the file or the URL where the key is located:

```
user@switch> request system license add filename |url
```

- To add a license key from the terminal:

```
user@switch> request system license add terminal
```

2. When prompted, enter the license key, separating multiple license keys with a blank line.

If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit the license entry mode.

A MACsec feature license is installed and maintained like any other switch license. See *Managing Licenses for the EX Series Switch (CLI Procedure)* or *Adding New Licenses (CLI Procedure)* for more detailed information on configuring and managing your MACsec software license.

Configuring the PIC Mode of the MACsec-capable Interfaces (EX4200 switches only)

To configure MACsec on an EX4200 switch, you must install the SFP+ MACsec uplink module. The interfaces on the SFP+ MACsec uplink module are the only MACsec-capable interfaces available for EX4200 switches. All four ports on the uplink module are MACsec-capable.

The SFP+ MACsec uplink module provides two ports for 10-gigabit small form-factor pluggable (SFP+) transceivers when configured to operate in 10-gigabit mode or four ports for 1-gigabit small form-factor pluggable (SFP) transceivers when configured to operate in 1-gigabit mode.

The PIC mode is set to **10g**, by default. You only need to perform this procedure if you want to operate your uplink in 1-gigabit mode, or if you previously set the uplink module to 1-gigabit mode and would like to return it to 10-gigabit mode.

To configure the PIC mode:

```
[edit chassis]
user@switch# set fpc fpc-slot-number pic 1 sfplus pic-mode (1g | 10g)
```

where **fpc-slot-number** is the FPC slot number, **pic-slot-number** is the PIC slot number, and the **[1g | 10g]** option configures the MACsec capability of the four SFP+ ports on the MACsec uplink module.

The **fpc-slot-number** is always 0 on standalone EX4200 switches, and is the member ID of the member switch in an EX4200 Virtual Chassis.

The PIC slot number is always 1 for the uplink module port slot on an EX4200 switch, so **pic 1** is always the specified PIC slot number.

The PIC mode is set to **10g** by default. When the PIC mode is set to **10g**, uplink ports 0 and 2 on the MACsec uplink module support MACsec at 10-Gbps speeds. Ports 1 and 3 cannot be used to send any traffic.

When the PIC mode is set to **1g**, all four SFP+ ports on the MACsec uplink module support MACsec at 1-Gbps speeds.

Configuring MACsec Using Static Connectivity Association Key Security Mode (Recommended for Enabling MACsec on Switch-to-Switch Links)

You can enable MACsec using static connectivity association key (CAK) security mode or static secure association keys (SAK) security mode on a point-to-point Ethernet link connecting switches. This procedure shows you how to configure MACsec using static CAK security mode.



BEST PRACTICE: We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

When you enable MACsec using static CAK security mode, a pre-shared key is exchanged between the switches on each end of the point-to-point Ethernet link. The pre-shared key includes a connectivity association name (CKN) and a connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

After the pre-shared keys are exchanged and verified, the MACsec Key Agreement (MKA) protocol, which enables and maintains MACsec on the link, is enabled. The MKA is responsible for selecting one of the two switches on the point-to-point link as the key server. The key server then creates a randomized security key that is shared only with the other device over the MACsec-secured link. The randomized security key enables and maintains MACsec on the point-to-point link. The key server will continue to periodically create and share a randomly-created security key over the point-to-point link for as long as MACsec is enabled.



NOTE: If the MACsec session is terminated due to a link failure, when the link is restored, the MKA key server elects a key server and generates a new SAK.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels—one for inbound traffic and one for outbound traffic—are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

To configure MACsec using static CAK security mode to secure a switch-to-switch Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1
```

2. Configure the MACsec security mode as **static-cak** for the connectivity association:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name security-mode
static-cak
```

For instance, to configure the MACsec security mode to **static-cak** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 security-mode static-cak
```

3. Create the pre-shared key by configuring the connectivity association key name (CKN) and connectivity association key (CAK):

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name pre-shared-key
ckn hexadecimal-number
user@switch# set connectivity-association connectivity-association-name pre-shared-key
cak hexadecimal-number
```

A pre-shared key is exchanged between directly-connected links to establish a MACsec-secure link. The pre-shared-key includes the CKN and the CAK. The CKN is a 64-digit hexadecimal number and the CAK is a 32-digit hexadecimal number. The CKN and the CAK must match on both ends of a link to create a MACsec-secured link.



NOTE: To maximize security, we recommend configuring all 64 digits of a CKN and all 32 digits of a CAK.

If you do not configure all 64 digits of a CKN or all 32 digits of a CAK, all remaining digits will be auto-configured to 0. However, you will receive a warning message when you commit the configuration.

After the pre-shared keys are successfully exchanged and verified by both ends of the link, the MACsec Key Agreement (MKA) protocol is enabled and manages the secure link. The MKA protocol then elects one of the two directly-connected switches as the key server. The key server then shares a random security with the other device over the MACsec-secure point-to-point link. The key server will continue to periodically create and share a random security key with the other device over the MACsec-secured point-to-point link as long as MACsec is enabled.

To configure a CKN of

37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311 and CAK of 228ef255aa23ff6729ee664acb66e91f on connectivity association ca1:

```
[edit security macsec]
user@switch# set connectivity-association ca1 pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@switch# set connectivity-association ca1 pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```



NOTE: MACsec is not enabled until a connectivity association is attached to an interface. See the final step of this procedure to attach a connectivity association to an interface.

4. (Required on non-EX4300 switches when connecting to EX4300 switches only)

Enable SCI tagging:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set include-sci
```

You must enable SCI tagging on a switch that is enabling MACsec on an Ethernet link connecting to an EX4300 switch.

SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. This option is, therefore, not available on EX4300 switches.

You should only use this option when enabling MACsec on a link to an EX4300 switch. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16.

If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
```

```
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association `ca1`:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower *interval* increases bandwidth overhead on the link; a higher *interval* optimizes MKA protocol communication.

The default *interval* is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link when MACsec using static CAK security mode is enabled.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association `ca1` is attached to an interface:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using static CAK security mode, by default.

When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named `ca1`:

```
[edit security macsec connectivity-association ca1]
user@switch# set offset 30
```


The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an **offset** is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link.

When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
```

```
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association ca1 to interface xe-0/0/1:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca1
```



NOTE: On an EX4300 uplink module, the first transceiver plugged into the uplink module determines the PIC mode, as the PIC recognizes the SFP type and programs all of the ports to be either ge- or xe-. Make sure the MACsec configuration on the interface matches the link speed for the uplink module ports.

MACsec using static CAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and contains pre-shared keys that match on both ends of the link.

See Also • [Understanding Media Access Control Security \(MACsec\) on page 217](#)

Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link

Before you begin to enable MACsec on a switch-to-host link:

- Confirm that MACsec on switch-to-host links is supported on your switch. See [“Understanding Media Access Control Security \(MACsec\)” on page 217](#).
- Configure a RADIUS server. The RADIUS server:
 - must be configured as the user database for 802.1X authentication.
 - Starting in Junos OS Release 15.1, the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework is required for MACsec on a switch-to-host link.
 - must have connectivity to the switch and to the host. The RADIUS server can be multiple hops from the switch or the host.

See Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch.

- Enable MACsec on the host device.

The procedures for enabling MACsec on the host device varies by host device, and is beyond the scope of this document.

To configure MACsec using dynamic security mode to secure a switch-to-host Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named `ca-dynamic1`, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca-dynamic1
```

2. Configure the MACsec security mode as dynamic for the connectivity association:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name security-mode
dynamic
```

For instance, to configure the MACsec security mode to dynamic on connectivity association `ca-dynamic1`:

```
[edit security macsec]
user@switch# set connectivity-association ca-dynamic1 security-mode dynamic
```

3. (Optional) Configure the **must-secure** option:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name mka must-secure
```

When the **must-secure** option is enabled, all traffic that is not MACsec-secured that is received on the interface is dropped.

When the **must-secure** option is disabled, all traffic from devices that support MACsec is MACsec-secured while traffic received from devices that do not support MACsec is forwarded through the network.

The **must-secure** option is particularly useful in scenarios where multiple devices, such as a phone and a PC, are accessing the network through the same Ethernet interface. If one of the devices supports MACsec while the other device does not support MACsec, the device that doesn't support MACsec can continue to send and receive traffic over the network—provided the **must-secure** option is disabled—while traffic to and from the device that supports MACsec is MACsec-secured. In this scenario, traffic to the device that is not MACsec-secured must be VLAN-tagged.

The **must-secure** option is disabled, by default.

4. (Required only if the host device requires SCI tagging) Enable SCI tagging:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set include-sci
```

You should only use this option when connecting a switch to a host that requires SCI tags. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16. If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association ca1:

```
[edit security macsec connectivity-association ca-dynamic1]  
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]  
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower interval increases bandwidth overhead on the link; a higher interval optimizes MKA protocol communication.

The default interval is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association ca-dynamic1 is attached to an interface:

```
[edit security macsec connectivity-association ca-dynamic1]  
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using dynamic security mode, by default. When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set offset 30
```

The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an offset is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link. When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association `ca-dynamic1`:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.



BEST PRACTICE: We recommend that any protocol other than MACsec being used on the MACsec connection, such as LLDP, LACP, STP, or layer 3 routing protocols, should be excluded and moved outside of the MACsec tunnel.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface. For instance, to assign connectivity association `ca-dynamic1` to interface `xe-0/0/1`:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca-dynamic1
```



NOTE: On an EX4300 uplink module, the first transceiver plugged into the uplink module determines the PIC mode, as the PIC recognizes the SFP type and programs all of the ports to be either ge- or xe-. Make sure the MACsec configuration on the interface matches the link speed for the uplink module ports.

Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link

When you enable MACsec using static secure association key (SAK) security mode, one of up to two manually configured security keys is used to secure the point-to-point Ethernet link between the switches. All security key names and values are configured by the user; there is no key server or other tool that creates security keys. Security is maintained on the point-to-point Ethernet link by periodically rotating the security keys. Each security key name and value must have a corresponding matching value on the interface at the other end of the point-to-point Ethernet link to maintain MACsec on the link.

You configure static SAKs within secure channels when you are enabling MACsec using static SAK security mode. You configure secure channels within connectivity associations. A typical connectivity association for MACsec using static SAK security mode contains two secure channels—one for inbound traffic and one for outbound traffic—that have each been configured with two static SAKs. You must attach the connectivity association with the secure channel configurations to an interface to enable MACsec using static SAK security mode.

To configure MACsec on a switch-to-switch Ethernet link using static SAK security mode:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1
```

2. Configure the MACsec security mode as **static-sak** for the connectivity association:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name security-mode static-sak
```

For instance, to configure the MACsec security mode to **static-sak** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 security-mode static-sak
```

3. Create a secure channel within the connectivity association. You can skip this step if you are configuring an existing secure channel.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name
```

For instance, to create secure channel **sc1** in connectivity association **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1
```

4. Define the security associations and the static SAKs for the secure channel:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name security-association number key key-string
```

where the **security-association number** is a number between 0 and 3, and the *key-string* is a 32-digit key defined statically by the network administrator.

The key string is a 32-digit hexadecimal number. The key string and the security association must match on both sides of an Ethernet connection to secure traffic using MACsec.

A secure channel must have at least two security associations with unique key strings. MACsec uses a security associations to establish a secure communications link, and periodically rotates to a new security association to keep the link secure. MACsec, therefore, must have at least one backup security association and key at all times.

To create one secure channel with two security associations and keys, for example:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 security-association 0 key
d183c4002fa6fe3d2d9a852c20ab8412
user@switch# set connectivity-association ca1 secure-channel sc1 security-association 1 key
b976c7494ab6fe2f2d4c432a90fd90a8
```

5. Specify whether the secure channel should be applied to traffic entering or leaving the switch:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name direction [inbound | outbound]
```

where **inbound** applies the secure channel to traffic entering the switch, and **outbound** applies the secure channel to traffic leaving the switch.



NOTE: A secure channel can only be applied to traffic entering (inbound) or leaving (outbound) an interface on the switch.

If you need to configure MACsec using SAKs on inbound and outbound traffic on the same interface, you must configure a connectivity association with one secure channel for inbound traffic and a second secure channel for outbound traffic. The connectivity association is assigned to an interface later in this process.

For instance, to configure secure channel **sc1** to apply MACsec to incoming traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 direction inbound
```

To configure secure channel **sc2** to apply MACsec to outgoing traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc2 direction outbound
```

6. Specify a MAC address:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id mac-address mac-address
```

If you are configuring a MAC address on a secure channel in the outbound direction, you should specify the MAC address of the interface as the **mac-address**.

If you are configuring a MAC address on a secure channel in the inbound direction, you should specify the MAC address of the interface at the other end of the link as the **mac-address**.

The **mac-address** variables must match on the sending and receiving secure channel on each side of a link to enable MACsec using static SAK security mode.



NOTE: You can see the MAC address of an interface in the **show interfaces** output.

To configure MACsec to accept frames from MAC address **12:34:56:ab:cd:ef** on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id mac-address
12:34:56:ab:cd:ef
```

7. Specify a port:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id port-id port-id-number
```

The **port-id-number** variables must match on a sending and receiving secure channel on each side of a link to enable MACsec.



NOTE: The only requirement for port numbers in this implementation of MACsec is that they match on the sending and receiving ends of an Ethernet link. When the port numbers match, MACsec is enabled for all traffic on the connection.

To specify port ID 4 on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id port-id 4
```

8. (Optional) Enable encryption:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name encryption
```

You can enable MACsec without enabling encryption. If a secure channel is configured on an interface without encryption, traffic is forwarded across the Ethernet link in clear text, and you will be able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic on the link does not represent a security threat.

Encryption is disabled by default when you are enabling MACsec using static SAK security mode. To ensure all traffic traversing secure-channel **sc1** is encrypted:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 encryption
```

9. (Optional) Set an offset to send the first 30 or 50 octets in unencrypted plain text when encryption is enabled.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name offset [0 | 30 | 50]
```

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

The default offset is 0, so all traffic on the link is encrypted when the **encryption** option is enabled and an **offset** is not set.

To change the offset to 30 for secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 offset 30
```

10. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association ca1 to interface xe-0/0/1:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca1
```



NOTE: On an EX4300 uplink module, the first transceiver plugged into the uplink module determines the PIC mode, as the PIC recognizes the SFP type and programs all of the ports to be either ge- or xe-. Make sure the MACsec configuration on the interface matches the link speed for the uplink module ports.

MACsec using static SAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and the configuration match on both ends of the link.

See Also • [Understanding Media Access Control Security \(MACsec\) on page 217](#)

MACsec Examples

- [Configuring MACsec on EX, SRX and Fusion Devices on page 249](#)
- [Configuring Media Access Control Security \(MACsec\) on MX Series Routers on page 268](#)
- [Example: Configuring MACsec over an MPLS CCC on EX Series Switches on page 281](#)
- [Example: Configuring MACsec over an MPLS CCC on MX Series Routers on page 304](#)

Configuring MACsec on EX, SRX and Fusion Devices

Media Access Control Security (MACsec) is an industry-standard security technology that provides secure communication for almost all types of traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly-connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec is standardized in IEEE 802.1AE.

You can configure MACsec to secure point-to-point Ethernet links connecting EX Series or QFX Series switches, or on Ethernet links connecting a switch to a host device such as a PC, phone, or server. Each point-to-point Ethernet link that you want to secure using MACsec must be configured independently. You can enable MACsec on switch-to-switch links using static secure association key (SAK) security mode or static connectivity association key (CAK) security mode. Both processes are provided in this document.



BEST PRACTICE: We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

The configuration steps for both processes are provided in this document.



BEST PRACTICE: When enabling MACsec, we recommend that when you examine your interface MTU, adjusting it for MACsec overhead, which is 32 bytes.



NOTE: This topic pertains to switches that support MACsec. Any specifics about a particular switch are identified as such.

- [Acquiring and Downloading the Junos OS Software on page 250](#)
- [Acquiring and Downloading the MACsec Feature License on page 251](#)
- [Configuring the PIC Mode of the MACsec-capable Interfaces \(EX4200 switches only\) on page 252](#)
- [Configuring MACsec Using Static Connectivity Association Key Security Mode \(Recommended for Enabling MACsec on Switch-to-Switch Links\) on page 254](#)
- [Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link on page 259](#)
- [Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link on page 264](#)

Acquiring and Downloading the Junos OS Software

For Junos OS Release 16.1 and later, you must download the standard Junos image to enable MACsec. MACsec is not supported in the limited image.

For releases prior to Junos OS Release 16.1, you must download the controlled version of your Junos OS software to enable MACsec. MACsec support is not available in the domestic version of Junos OS software in releases prior to Junos OS Release 15.1.

You can identify whether a software package is the standard or controlled version of Junos OS by viewing the package name. A software package for a controlled version of Junos OS is named using the following format:

```
package-name-m.nZx.y-controlled-signed.tgz
```

A software package for a standard version of Junos OS is named using the following format:

```
package-name-m.nZx.y-.tgz
```

If you are unsure which version of Junos OS is running on your switch, enter the **show version** command. If the **JUNOS Crypto Software Suite** description appears in the output, you are running the controlled version of Junos OS. If you are running a controlled version of Junos OS, enter the **show system software** command to display the version. The output also shows the version of all loaded software packages.

The controlled version of Junos OS software for EX Series or QFX Series switches contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS software is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring the controlled version of your Junos OS software, contact Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

The standard version of Junos OS software for EX Series and QFX Series switches contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of this Junos OS software is strictly controlled under United States export laws. The export, import, and use of this Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring this version of your Junos OS software, contact Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

The process for installing the controlled or standard version of Junos OS software onto your switch is identical to installing any other version of Junos OS software. You must enter the **request system software add** statement to download the Junos OS image, and the **request system reboot** statement to reboot the switch to complete the upgrade procedure.

See “[Understanding Media Access Control Security \(MACsec\)](#)” on page 217 for additional information on the versions of Junos OS software that are required for MACsec.

Acquiring and Downloading the MACsec Feature License

A feature license is required to configure MACsec on an EX Series or a QFX Series switch, with the exception of the QFX10000-6C-DWDM and QFX10000-30C-M line cards. If the MACsec licence is not installed, MACsec functionality cannot be activated.

The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series or QFX Series switches cannot be purchased to enable MACsec.

To purchase a software license for MACsec, contact your Juniper Networks sales representative (<https://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key. You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

For a Virtual Chassis deployment, two MACsec license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role.

To add one or more new MACsec license keys on the switch, follow this procedure:

1. Add the license key or keys:
 - To add one or more license keys from a file or URL, specify the filename of the file or the URL where the key is located:

```
user@switch> request system license add filename |url
```

- To add a license key from the terminal:

```
user@switch> request system license add terminal
```

2. When prompted, enter the license key, separating multiple license keys with a blank line.

If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit the license entry mode.

A MACsec feature license is installed and maintained like any other switch license. See *Managing Licenses for the EX Series Switch (CLI Procedure)* or *Adding New Licenses (CLI Procedure)* for more detailed information on configuring and managing your MACsec software license.

Configuring the PIC Mode of the MACsec-capable Interfaces (EX4200 switches only)

To configure MACsec on an EX4200 switch, you must install the SFP+ MACsec uplink module. The interfaces on the SFP+ MACsec uplink module are the only MACsec-capable interfaces available for EX4200 switches. All four ports on the uplink module are MACsec-capable.

The SFP+ MACsec uplink module provides two ports for 10-gigabit small form-factor pluggable (SFP+) transceivers when configured to operate in 10-gigabit mode or four ports for 1-gigabit small form-factor pluggable (SFP) transceivers when configured to operate in 1-gigabit mode.

The PIC mode is set to **10g**, by default. You only need to perform this procedure if you want to operate your uplink in 1-gigabit mode, or if you previously set the uplink module to 1-gigabit mode and would like to return it to 10-gigabit mode.

To configure the PIC mode:

```
[edit chassis]  
user@switch# set fpc fpc-slot-number pic 1 sfpplus pic-mode (1g | 10g)
```

where **fpc-slot-number** is the FPC slot number, **pic-slot-number** is the PIC slot number, and the **[1g | 10g]** option configures the MACsec capability of the four SFP+ ports on the MACsec uplink module.

The **fpc-slot-number** is always 0 on standalone EX4200 switches, and is the member ID of the member switch in an EX4200 Virtual Chassis.

The PIC slot number is always 1 for the uplink module port slot on an EX4200 switch, so **pic 1** is always the specified PIC slot number.

The PIC mode is set to **10g** by default. When the PIC mode is set to **10g**, uplink ports 0 and 2 on the MACsec uplink module support MACsec at 10-Gbps speeds. Ports 1 and 3 cannot be used to send any traffic.

When the PIC mode is set to **1g**, all four SFP+ ports on the MACsec uplink module support MACsec at 1-Gbps speeds.

Configuring MACsec Using Static Connectivity Association Key Security Mode (Recommended for Enabling MACsec on Switch-to-Switch Links)

You can enable MACsec using static connectivity association key (CAK) security mode or static secure association keys (SAK) security mode on a point-to-point Ethernet link connecting switches. This procedure shows you how to configure MACsec using static CAK security mode.



BEST PRACTICE: We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

When you enable MACsec using static CAK security mode, a pre-shared key is exchanged between the switches on each end of the point-to-point Ethernet link. The pre-shared key includes a connectivity association name (CKN) and a connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

After the pre-shared keys are exchanged and verified, the MACsec Key Agreement (MKA) protocol, which enables and maintains MACsec on the link, is enabled. The MKA is responsible for selecting one of the two switches on the point-to-point link as the key server. The key server then creates a randomized security key that is shared only with the other device over the MACsec-secured link. The randomized security key enables and maintains MACsec on the point-to-point link. The key server will continue to periodically create and share a randomly-created security key over the point-to-point link for as long as MACsec is enabled.



NOTE: If the MACsec session is terminated due to a link failure, when the link is restored, the MKA key server elects a key server and generates a new SAK.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels—one for inbound traffic and one for outbound traffic—are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

To configure MACsec using static CAK security mode to secure a switch-to-switch Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1
```

2. Configure the MACsec security mode as **static-cak** for the connectivity association:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name security-mode
static-cak
```

For instance, to configure the MACsec security mode to **static-cak** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 security-mode static-cak
```

3. Create the pre-shared key by configuring the connectivity association key name (CKN) and connectivity association key (CAK):

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name pre-shared-key
ckn hexadecimal-number
user@switch# set connectivity-association connectivity-association-name pre-shared-key
cak hexadecimal-number
```

A pre-shared key is exchanged between directly-connected links to establish a MACsec-secure link. The pre-shared-key includes the CKN and the CAK. The CKN is a 64-digit hexadecimal number and the CAK is a 32-digit hexadecimal number. The CKN and the CAK must match on both ends of a link to create a MACsec-secured link.



NOTE: To maximize security, we recommend configuring all 64 digits of a CKN and all 32 digits of a CAK.

If you do not configure all 64 digits of a CKN or all 32 digits of a CAK, all remaining digits will be auto-configured to 0. However, you will receive a warning message when you commit the configuration.

After the pre-shared keys are successfully exchanged and verified by both ends of the link, the MACsec Key Agreement (MKA) protocol is enabled and manages the secure link. The MKA protocol then elects one of the two directly-connected switches as the key server. The key server then shares a random security with the other device over the MACsec-secure point-to-point link. The key server will continue to periodically create and share a random security key with the other device over the MACsec-secured point-to-point link as long as MACsec is enabled.

To configure a CKN of

37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311 and CAK of 228ef255aa23ff6729ee664acb66e91f on connectivity association ca1:

```
[edit security macsec]
user@switch# set connectivity-association ca1 pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@switch# set connectivity-association ca1 pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```



NOTE: MACsec is not enabled until a connectivity association is attached to an interface. See the final step of this procedure to attach a connectivity association to an interface.

4. (Required on non-EX4300 switches when connecting to EX4300 switches only)

Enable SCI tagging:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set include-sci
```

You must enable SCI tagging on a switch that is enabling MACsec on an Ethernet link connecting to an EX4300 switch.

SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. This option is, therefore, not available on EX4300 switches.

You should only use this option when enabling MACsec on a link to an EX4300 switch. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16.

If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
```

```
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association `ca1`:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower *interval* increases bandwidth overhead on the link; a higher *interval* optimizes MKA protocol communication.

The default *interval* is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link when MACsec using static CAK security mode is enabled.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association `ca1` is attached to an interface:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using static CAK security mode, by default.

When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named `ca1`:

```
[edit security macsec connectivity-association ca1]
user@switch# set offset 30
```

The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an **offset** is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link.

When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]  
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
```

```
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association ca1 to interface xe-0/0/1:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca1
```



NOTE: On an EX4300 uplink module, the first transceiver plugged into the uplink module determines the PIC mode, as the PIC recognizes the SFP type and programs all of the ports to be either ge- or xe-. Make sure the MACsec configuration on the interface matches the link speed for the uplink module ports.

MACsec using static CAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and contains pre-shared keys that match on both ends of the link.

See Also • [Understanding Media Access Control Security \(MACsec\) on page 217](#)

Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link

Before you begin to enable MACsec on a switch-to-host link:

- Confirm that MACsec on switch-to-host links is supported on your switch. See [“Understanding Media Access Control Security \(MACsec\)” on page 217](#).
- Configure a RADIUS server. The RADIUS server:
 - must be configured as the user database for 802.1X authentication.
 - Starting in Junos OS Release 15.1, the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework is required for MACsec on a switch-to-host link.
 - must have connectivity to the switch and to the host. The RADIUS server can be multiple hops from the switch or the host.

See *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*.

- Enable MACsec on the host device.

The procedures for enabling MACsec on the host device varies by host device, and is beyond the scope of this document.

To configure MACsec using dynamic security mode to secure a switch-to-host Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named `ca-dynamic1`, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca-dynamic1
```

2. Configure the MACsec security mode as dynamic for the connectivity association:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name security-mode
dynamic
```

For instance, to configure the MACsec security mode to dynamic on connectivity association `ca-dynamic1`:

```
[edit security macsec]
user@switch# set connectivity-association ca-dynamic1 security-mode dynamic
```

3. (Optional) Configure the **must-secure** option:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name mka must-secure
```

When the **must-secure** option is enabled, all traffic that is not MACsec-secured that is received on the interface is dropped.

When the **must-secure** option is disabled, all traffic from devices that support MACsec is MACsec-secured while traffic received from devices that do not support MACsec is forwarded through the network.

The **must-secure** option is particularly useful in scenarios where multiple devices, such as a phone and a PC, are accessing the network through the same Ethernet interface. If one of the devices supports MACsec while the other device does not support MACsec, the device that doesn't support MACsec can continue to send and receive traffic over the network—provided the **must-secure** option is disabled—while traffic to and from the device that supports MACsec is MACsec-secured. In this scenario, traffic to the device that is not MACsec-secured must be VLAN-tagged.

The **must-secure** option is disabled, by default.

4. (Required only if the host device requires SCI tagging) Enable SCI tagging:


```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set include-sci
```

You should only use this option when connecting a switch to a host that requires SCI tags. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16. If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association ca1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower interval increases bandwidth overhead on the link; a higher interval optimizes MKA protocol communication.

The default interval is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association ca-dynamic1 is attached to an interface:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using dynamic security mode, by default. When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]  
user@switch# set offset 30
```

The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an offset is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]  
user@switch# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link. When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association `ca-dynamic1`:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.



BEST PRACTICE: We recommend that any protocol other than MACsec being used on the MACsec connection, such as LLDP, LACP, STP, or layer 3 routing protocols, should be excluded and moved outside of the MACsec tunnel.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface. For instance, to assign connectivity association `ca-dynamic1` to interface `xe-0/0/1`:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca-dynamic1
```



NOTE: On an EX4300 uplink module, the first transceiver plugged into the uplink module determines the PIC mode, as the PIC recognizes the SFP type and programs all of the ports to be either ge- or xe-. Make sure the MACsec configuration on the interface matches the link speed for the uplink module ports.

Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link

When you enable MACsec using static secure association key (SAK) security mode, one of up to two manually configured security keys is used to secure the point-to-point Ethernet link between the switches. All security key names and values are configured by the user; there is no key server or other tool that creates security keys. Security is maintained on the point-to-point Ethernet link by periodically rotating the security keys. Each security key name and value must have a corresponding matching value on the interface at the other end of the point-to-point Ethernet link to maintain MACsec on the link.

You configure static SAKs within secure channels when you are enabling MACsec using static SAK security mode. You configure secure channels within connectivity associations. A typical connectivity association for MACsec using static SAK security mode contains two secure channels—one for inbound traffic and one for outbound traffic—that have each been configured with two static SAKs. You must attach the connectivity association with the secure channel configurations to an interface to enable MACsec using static SAK security mode.

To configure MACsec on a switch-to-switch Ethernet link using static SAK security mode:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1
```

2. Configure the MACsec security mode as **static-sak** for the connectivity association:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name security-mode
static-sak
```

For instance, to configure the MACsec security mode to **static-sak** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 security-mode static-sak
```

3. Create a secure channel within the connectivity association. You can skip this step if you are configuring an existing secure channel.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name
```

For instance, to create secure channel **sc1** in connectivity association **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1
```

4. Define the security associations and the static SAKs for the secure channel:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name security-association number key key-string
```

where the **security-association** *number* is a number between 0 and 3, and the *key-string* is a 32-digit key defined statically by the network administrator.

The key string is a 32-digit hexadecimal number. The key string and the security association must match on both sides of an Ethernet connection to secure traffic using MACsec.

A secure channel must have at least two security associations with unique key strings. MACsec uses a security associations to establish a secure communications link, and periodically rotates to a new security association to keep the link secure. MACsec, therefore, must have at least one backup security association and key at all times.

To create one secure channel with two security associations and keys, for example:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 security-association 0 key
d183c4002fa6fe3d2d9a852c20ab8412
user@switch# set connectivity-association ca1 secure-channel sc1 security-association 1 key
b976c7494ab6fe2f2d4c432a90fd90a8
```

5. Specify whether the secure channel should be applied to traffic entering or leaving the switch:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name direction [inbound | outbound]
```

where **inbound** applies the secure channel to traffic entering the switch, and **outbound** applies the secure channel to traffic leaving the switch.



NOTE: A secure channel can only be applied to traffic entering (inbound) or leaving (outbound) an interface on the switch.

If you need to configure MACsec using SAKs on inbound and outbound traffic on the same interface, you must configure a connectivity association with one secure channel for inbound traffic and a second secure channel for outbound traffic. The connectivity association is assigned to an interface later in this process.

For instance, to configure secure channel **sc1** to apply MACsec to incoming traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 direction inbound
```

To configure secure channel **sc2** to apply MACsec to outgoing traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc2 direction outbound
```

6. Specify a MAC address:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id mac-address mac-address
```

If you are configuring a MAC address on a secure channel in the outbound direction, you should specify the MAC address of the interface as the **mac-address**.

If you are configuring a MAC address on a secure channel in the inbound direction, you should specify the MAC address of the interface at the other end of the link as the **mac-address**.

The **mac-address** variables must match on the sending and receiving secure channel on each side of a link to enable MACsec using static SAK security mode.



NOTE: You can see the MAC address of an interface in the **show interfaces** output.

To configure MACsec to accept frames from MAC address **12:34:56:ab:cd:ef** on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id mac-address
12:34:56:ab:cd:ef
```

7. Specify a port:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id port-id port-id-number
```

The **port-id-number** variables must match on a sending and receiving secure channel on each side of a link to enable MACsec.



NOTE: The only requirement for port numbers in this implementation of MACsec is that they match on the sending and receiving ends of an Ethernet link. When the port numbers match, MACsec is enabled for all traffic on the connection.

To specify port ID 4 on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id port-id 4
```

8. (Optional) Enable encryption:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name encryption
```

You can enable MACsec without enabling encryption. If a secure channel is configured on an interface without encryption, traffic is forwarded across the Ethernet link in clear text, and you will be able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic on the link does not represent a security threat.

Encryption is disabled by default when you are enabling MACsec using static SAK security mode. To ensure all traffic traversing secure-channel **sc1** is encrypted:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 encryption
```

9. (Optional) Set an offset to send the first 30 or 50 octets in unencrypted plain text when encryption is enabled.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name offset [0 | 30 | 50]
```

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

The default offset is 0, so all traffic on the link is encrypted when the **encryption** option is enabled and an **offset** is not set.

To change the offset to 30 for secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 offset 30
```

10. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association ca1 to interface xe-0/0/1:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca1
```



NOTE: On an EX4300 uplink module, the first transceiver plugged into the uplink module determines the PIC mode, as the PIC recognizes the SFP type and programs all of the ports to be either ge- or xe-. Make sure the MACsec configuration on the interface matches the link speed for the uplink module ports.

MACsec using static SAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and the configuration match on both ends of the link.

Release History Table

Release	Description
15.1	Starting in Junos OS Release 15.1, the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework is required for MACsec on a switch-to-host link.

Related Documentation

- [Understanding Media Access Control Security \(MACsec\) on page 217](#)

Configuring Media Access Control Security (MACsec) on MX Series Routers

Media Access Control Security (MACsec) is an industry-standard security technology that provides secure communication for almost all types of traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly-connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec is standardized in IEEE 802.1AE.

Starting with Junos OS Release 15.1, you can configure MACsec to secure point-to-point Ethernet links connecting MX Series routers with MACsec-capable MICs, or on Ethernet links connecting a switch to a host device such as a PC, phone, or server. Each

point-to-point Ethernet link that you want to secure using MACsec must be configured independently. You can enable MACsec on router-to-router links using static connectivity association key (CAK) security mode. The process is provided in this document.

Starting in Junos OS Release 14.2R2 and 15.1R1, you can configure Media Access Control Security (MACsec) on MX Series routers with the enhanced 20-port Gigabit Ethernet MIC (model number MIC-3D-20GE-SFP-E).

The configuration steps for both processes are provided in this document.

- [Configuring MACsec Using Static Connectivity Association Key Security Mode on page 270](#)
- [Configuring MACsec Using Preshared Key Hitless Rollover Keychain on MX-series Routers \(Recommended for Enabling MACsec on Router-to-Router Links\) on page 276](#)
- [Configuring MACsec Key Agreement Protocol in Fail Open Mode on MX2020 and MX2010 Routers on page 279](#)
- [Configuring MACsec with Fallback PSK on page 279](#)

Configuring MACsec Using Static Connectivity Association Key Security Mode

You can enable MACsec using static connectivity association key (CAK) security mode on a point-to-point Ethernet link connecting switches. This procedure shows you how to configure MACsec using static CAK security mode.

When you enable MACsec using static CAK security mode, a preshared key is exchanged between the switches on each end of the point-to-point Ethernet link. The preshared key includes a connectivity association name (CKN) and a connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

After the preshared keys are exchanged and verified, the MACsec Key Agreement (MKA) protocol, which enables and maintains MACsec on the link, is enabled. The MKA is responsible for selecting one of the two switches on the point-to-point link as the key server. The key server then creates a randomized security key that is shared only with the other device over the MACsec-secured link. The randomized security key enables and maintains MACsec on the point-to-point link. The key server will continue to periodically create and share a randomly-created security key over the point-to-point link for as long as MACsec is enabled.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels— one for inbound traffic and one for outbound traffic— are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

To configure MACsec using static CAK security mode to secure a router-to-router Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@host# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named **ca1**, enter:

```
[edit security macsec]
user@host# set connectivity-association ca1
```

2. Configure the MACsec security mode as **static-cak** for the connectivity association:

```
[edit security macsec]
user@host# set connectivity-association connectivity-association-name security-mode
static-cak
```

For instance, to configure the MACsec security mode to **static-cak** on connectivity association **ca1**:

```
[edit security macsec]
user@host# set connectivity-association ca1 security-mode static-cak
```

3. Create the preshared key by configuring the connectivity association key name (CKN) and connectivity association key (CAK):

```
[edit security macsec]
user@host# set connectivity-association connectivity-association-name pre-shared-key ckn hexadecimal-number
user@host# set connectivity-association connectivity-association-name pre-shared-key cak hexadecimal-number
```

A preshared key is exchanged between directly-connected links to establish a MACsec-secure link. The preshared-key includes the CKN and the CAK. The CKN is a 64-digit hexadecimal number and the CAK is a 32-digit hexadecimal number. The CKN and the CAK must match on both ends of a link to create a MACsec-secured link.



NOTE: To maximize security, we recommend configuring all 64 digits of a CKN and all 32 digits of a CAK.

If you do not configure all 64 digits of a CKN or all 32 digits of a CAK, however, all remaining digits will be auto-configured to 0.

After the preshared keys are successfully exchanged and verified by both ends of the link, the MACsec Key Agreement (MKA) protocol is enabled and manages the secure link. The MKA protocol then elects one of the two directly-connected switches as the key server. The key server then shares a random security with the other device over the MACsec-secure point-to-point link. The key server will continue to periodically create and share a random security key with the other device over the MACsec-secured point-to-point link as long as MACsec is enabled.

To configure a CKN of 37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311 and CAK of 228ef255aa23ff6729ee664acb66e91f on connectivity association ca1:

```
[edit security macsec]
user@host# set connectivity-association ca1 pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@host# set connectivity-association ca1 pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```



NOTE:

- MACsec is not enabled until a connectivity association is attached to an interface. See the final step of this procedure to attach a connectivity association to an interface.
- In FIPS mode, instead of using `set connectivity-association ca1 pre-shared-key cak` command, you must use the following command:

```
user@host# prompt connectivity-association ca1 pre-shared-key cak
```

4. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@host# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16.

If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]  
user@host# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]  
user@host# set mka key-server-priority 255
```

5. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@host# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower *interval* increases bandwidth overhead on the link; a higher *interval* optimizes MKA protocol communication.

The default *interval* is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link when MACsec using static CAK security mode is enabled.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association **ca1** is attached to an interface:

```
[edit security macsec connectivity-association ca1]  
user@host# set mka transmit-interval 6000
```

6. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@host# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using static CAK security mode, by default.

When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

7. Assign an Encryption Algorithm

You can encrypt all traffic entering or leaving the interface using any of the following MACsec encryption algorithms:

- gcm-aes-128— GCM-AES-128 cipher suite without extended packet numbering (XPN) mode
- gcm-aes-256— GCM-AES-256 cipher suite without XPN
- gcm-aes-xpn-128— GCM-AES-XPN_128 cipher suite with XPN mode
- gcm-aes-xpn-256— GCM-AES-XPN_256 cipher suite with XPN mode

If MACsec encryption is enabled and if no encryption algorithm is specified, the default (gcm-aes-128) encryption algorithm is used without XPN mode.



NOTE:

- The encryption algorithms with XPN mode are not supported on MX-series MPC7E-10G routers.
- Only GCM-AES-128 is supported on MIC-3D-20GE-SFP-E and MIC-3D-20GE-SFP-EH.

```
[edit security macsec connectivity-association connectivity-association-name]
user@host# set cipher-suite (gcm-aes-128 | gcm-aes-256 | gcm-aes-xpn-128 |
gcm-aes-xpn-256)
```

For instance, if you wanted to encrypt using gcm-aes-xpn-128 algorithm in the connectivity association named **ca1**:

```
[edit security macsec connectivity-association ca1]
user@host# set cipher-suite gcm-aes-xpn-128
```

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]
user@host# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named **ca1**:

```
[edit security macsec connectivity-association ca1]
user@host# set offset 30
```

The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an **offset** is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]  
user@host# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link.

When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]  
user@host# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]  
user@host# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
```

```
user@host# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol— in this case, LLDP— that are sent or received on the link.

11. Assign the connectivity association to an interface:



NOTE: Starting in Junos OS Release 16.1R2, when Media Access Control Security (MACsec) is enabled on an interface, the interface flow control capability is enabled by default, regardless of the configuration that you set using the (flow-control | no-flow-control) statement at the [edit interfaces *interface-name* gigether-options] hierarchy level. When MACsec is disabled, interface flow control is restored to the configuration that you set using the flow-control statement at the [edit interfaces] hierarchy level. When MACsec is enabled, additional header bytes are added to the packet by the MACsec PHY. With line rate traffic, when MACsec is enabled and flow control is disabled, the pause frames sent by the MACsec PHY are terminated by the MIC's MAC (enhanced 20-port Gigabit Ethernet MICs on MX Series routers) and not transferred to the Packet Forwarding Engine, causing framing errors. Therefore, when MACsec is enabled on an interface, flow control is also automatically enabled on such an interface.

```
[edit security macsec]
user@host# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association ca1 to interface ge-0/0/1:

```
[edit security macsec]
user@host# set interfaces ge-0/0/1 connectivity-association ca1
```

MACsec using static CAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and contains preshared keys that match on both ends of the link.

See Also • [Understanding Media Access Control Security \(MACsec\) on page 217](#)

Configuring MACsec Using Preshared Key Hitless Rollover Keychain on MX-series Routers (Recommended for Enabling MACsec on Router-to-Router Links)



NOTE: Although this feature is documented in Junos OS Release 17.4R1, it is still not supported. It will be available beginning with Junos OS Release 17.4R1 S1.

In the MACsec implementation using static connectivity association key (CAK) prior to release 17.4R1, the user is allowed to configure one static CAK for every connectivity association. Whenever CAK configuration changes, the MACsec session is dropped, resetting peer sessions or interrupting the routing protocol.

For increased security and to prevent session drops when the CAK configuration changes, the hitless rollover keychain feature is implemented. In this implementation, a key chain that has the multiple security keys, key names and start times is used. Each key in the keychain has a unique start time. At the next key's start time, a rollover occurs from the current key to the next key, and the next key becomes the current key. With the implementation of the hitless rollover keychain feature, the MACsec Key Agreement (MKA) protocol establishes MACsec sessions successfully without any session drop when the CAK configuration changes.

For a successful MACsec configuration using preshared key (PSK) hitless rollover keychain:

- The keychain names, keys and start time of each key must be the same in both the participating nodes.
- The order of the keychain names, keys and start time must be same in both the participating nodes.
- The time must be synchronized in the participating nodes.

The existing **authentication-key-chains** and **macsec connectivity-association** commands are used for implementing hitless rollover keychain with the addition of two new attributes:

- **key-name**—Authentication key name, and this **key-name** is used as the CKN for MACsec.
- **pre-shared-key-chain**—The preshared connectivity association keychain name.

To secure a router-to-router Ethernet link by using MACsec with PSK hitless rollover keychain configuration:



NOTE: Ensure that you execute the following steps in both the participating nodes in the same order.

1. Synchronize the time in the participating nodes to the same NTP server.

```
user@host# set date ntp servers
```

For instance, to set the date and time as per the NTP server 192.168.40.1, enter:

```
user@host# set date ntp 192.168.40.1
```

2. Configure a set of PSKs in a keychain. A keychain consists of a security key, key name, and start time.

To configure a keychain:

- a. Create the secret password to use. It is a string of hexadecimal digits up to 64 characters long. The password can include spaces if the character string is enclosed in quotation marks. The keychain's secret-data is used as a CAK.

```
[edit]
```

```
user@host# set security authentication-key-chains key-chain key-chain-name key key  
secret secret-data
```

For instance, to create the secret password 01112233445566778899aabbccddeeff for the keychain macsec_key_chain and key 1, enter:

```
[edit]
```

```
user@host# set security authentication-key-chains key-chain macsec_key_chain key 1  
secret 01112233445566778899aabbccddeeff
```

- b. Configure the authentication key name. It is a string of hexadecimal digits up to 32 characters long.

```
[edit]
```

```
user@host# set security authentication-key-chains key-chain macsec_key_chain key key  
key-name authentication_key_name
```

For instance, to create the key name 01112233445566778899aabbccddeefe, enter:

```
[edit]
```

```
user@host# set security authentication-key-chains key-chain macsec_key_chain key 1  
key-name 01112233445566778899aabbccddeefe
```

- c. Configure the time when the preshared rollover keychain starts.

```
[edit]
```

```
user@host# set security authentication-key-chains key-chain macsec_key_chain key key  
start-time "PSK keychain rollover start time"
```

For instance, if you want the key name with 01112233445566778899aabbccddeefe to start rollover at 2017-12-18.20:55:00 +0000, enter:

```
[edit]
```

```
user@host# set security authentication-key-chains key-chain macsec_key_chain key 1  
start-time "2017-12-18.20:55:00 +0000"
```

3. Associate the newly created keychain with a MACsec connectivity association.

- a. Configure the MACsec security mode for the connectivity association.

```
[edit]
user@host# set security macsec connectivity-association connectivity-association-name
security-mode security-mode
```

For instance, to configure the connectivity association ca1 with security mode static-cak, enter:

```
[edit]
user@host# set security macsec connectivity-association ca1 security-mode static-cak
```

- b. Associate the preshared keychain name with the connectivity association.

```
[edit]
user@host# set security macsec connectivity-association connectivity-association-name
pre-shared-key-chain macsec-key-chain-name
```

For instance, if you want to associate the keychain name macsec_key_chain with the connectivity association ca1, enter:

```
[edit security macsec]
user@host# set security macsec connectivity-association ca1 pre-shared-key-chain
macsec_key_chain
```

4. Assign the configured connectivity association with a specified MACsec interface.

```
[edit]
user@host# set security macsec interfaces interface-name connectivity-association
connectivity-association-name
```

For instance, to assign the connectivity association ca1 to the interface ge-0/0/1:

```
[edit]
user@host# set security macsec interfaces ge-0/0/1 connectivity-association ca1
```

Configuring MACsec Key Agreement Protocol in Fail Open Mode on MX2020 and MX2010 Routers

In the MACsec implementation in static CAK mode (prior to release 17.4R1), MACsec Key Agreement (MKA) protocol does not allow transmission (ingress or egress) of cleartext messages with or without secure channels. If an MKA session is not established, the data is dropped.

Service providers prioritize network availability over information security. Starting with Junos OS Release 17.4R1, transmission of clear text data is possible with or without the MKA protocol session being established. A new configuration statement, **should-secure**, introduced in 17.4R1 makes the transmission of cleartext data possible. There can be two scenarios for data transmission with the introduction of the **should-secure** configuration statement:

- **should-secure** not configured

This is the default CAK mode for MACsec and in this mode, traffic is allowed to pass encrypted with MACsec headers only when the MKA session is established. If the MKA session is not established, all traffic is discarded except Extensible Authentication Protocol over LAN (EAPoL).

- **should-secure** configured

If **should-secure** is configured and if the MKA session is not established, traffic is still allowed in cleartext without the MACsec header. If the MKA session is established successfully, traffic is allowed with MACsec headers.

To configure the MKA Protocol in Fail Open Mode:

```
[edit security macsec connectivity-association connectivity-association-name]
user@host# set mka should-secure;
```

Configuring MACsec with Fallback PSK

When you enable MACsec using static CAK security mode, a preshared key (PSK) is exchanged between the devices on each end of the point-to-point Ethernet link. The PSK includes a connectivity association name (CKN) and a connectivity association key (CAK). The PSK must match across devices for a MACsec session to be established. If there is a mismatch, the session will not be established and all packets will be dropped.

You can configure a fallback PSK to prevent traffic loss in case the primary PSK fails to establish a connection. The fallback PSK is used when primary keys do not match for the initial MACsec negotiation.

If a MACsec session has already been established, and the primary PSK is changed on one device but not the other, the resulting mismatch is resolved by using the older primary PSK. The older primary PSK is a temporary key known as the preceding PSK.

With fallback PSK configured, a MACsec session can be secured with one of the following keys:

- Primary PSK (configurable)—The preferred key.

- Fallback PSK (configurable)—Used when the primary PSK fails to establish a MACsec session.
- Preceding PSK (non-configurable)—When a new primary PSK is configured, the old primary PSK becomes the preceding PSK.

The status of the CAK for each key can be either live, active or in-progress. See [Table 10 on page 280](#) for a description of each status.

Table 10: CAK status descriptions

CAK Status	Description
Live	<ul style="list-style-type: none"> • CAK has been validated by MKA. • MACsec session is live. • SAK is successfully generated using this key. • CAK is used for encryption and decryption of the MACsec session. • MKA hello packets are sent and received for this key at a configured interval.
Active	<ul style="list-style-type: none"> • CAK has been validated by MKA. • MACsec session is live. • SAK is not generated using this key. • CAK is not used for encryption and decryption of the MACsec session. • MKA hello packets are sent and received for this key at a configured interval.
In-progress	<ul style="list-style-type: none"> • No valid live or potential peer is found. • The MACsec session is in-progress to find a peer. • MKA hello packets are sent and received for this key at a configured interval.

A mismatch of keys occurs when a new PSK is configured on one side of the MACsec link and the other side is either misconfigured or not configured with the new key. The fallback behavior depends on which components of the PSK are changed (CAK, CKN, or both). Each mismatch scenario is described below:

- If the CAK is changed, and the CKN remains the same, the existing MACsec session will be disconnected. A new session will be initiated with the old CKN and new CAK value.
- If the CKN is changed, and the CAK remains the same, the old CKN paired with the existing CAK becomes the preceding PSK, and the session will be live with preceding PSK. A new session is initiated with the newly-created CKN and the CAK, which will be in-progress until the peer node is also configured with the same CKN.
- If both the CAK and the CKN are changed, the old CAK+CKN pair becomes the preceding PSK, and the session will be live with the preceding PSK. A new session is initiated with the new CAK+CKN pair, which will be in-progress until the peer node is also configured with the same CAK+CKN.



NOTE: The preceding PSK takes priority over the fallback PSK, so if the session is live with the preceding PSK, the fallback PSK will not take effect. If you want the session to be live with the fallback PSK, you must configure the `disable-preceding-key` statement.

Fallback PSK is supported for preshared keychains. You can configure a fallback PSK along with a preshared key, or with a preshared keychain. The preshared key and preshared keychain are mutually exclusive.

If only a fallback PSK is configured, and there is no primary PSK, both devices attempt to establish a session with the fallback PSK. If the session comes up, the SAK derived from this session is used for data traffic encryption. If the established session is broken, the devices continue attempting to reestablish the session and traffic will be dropped until the session is reestablished.

The fallback PSK is configured as part of the connectivity association (CA). The CA can be configured globally for all interfaces or on a per-interface basis, allowing different fallback keys for different interfaces.

To configure the fallback PSK, configure the CAK and the CKN as part of the CA:

```
[edit security macsec connectivity-association ca-name]
user@switch# set fallback-key cak key
user@switch# set fallback-key ckn key-name
```

The following restrictions apply to fallback PSK configuration:

- Fallback CAK and CKN should not match any key configured in the keychain under the same CA.
- Security mode configuration must be present to configure the fallback key.
- Key length restrictions for the configured cipher suite apply to the fallback CAK and CKN.

Example: Configuring MACsec over an MPLS CCC on EX Series Switches

This example shows how to enable MACsec to secure sensitive traffic traveling from a user at one site to a user at another site over a basic MPLS CCC.

- [Requirements on page 282](#)
- [Overview and Topology on page 282](#)
- [Configuring MPLS on page 285](#)
- [Configuring MACsec on page 292](#)
- [Configuring VLANs to Direct Traffic onto the MACsec-Secured CCC on page 296](#)
- [Verification on page 298](#)

Requirements

This example uses the following hardware and software components:

- Three EX4550 switches used as the PE and provider switches in the MPLS network
- One EX4550 switch used as the CE switch connecting site A to the MPLS network
- One EX4200 switch that has installed an SFP+ MACsec uplink module used as the CE switch connecting site B to the MPLS network
- Junos OS Release 12.2R1 or later running on all EX4550 switches in the MPLS network (PE1, PE2, or the provider switch)
- Junos OS Release 13.2X50-D15 (controlled version) or later running on the CE switch at site A and the CE switch at site B



NOTE: The controlled version of Juniper Networks Junos operating system (Junos OS) software must be downloaded to enable MACsec. MACsec software support is not available in the domestic version of Junos OS software, which is installed on the switch by default. The controlled version of Junos OS software includes all features and functionality available in the domestic version of Junos OS, while also supporting MACsec. See “[Understanding Media Access Control Security \(MACsec\)](#)” on page 217 for additional information about MACsec software requirements.

- A MACsec feature license installed on the CE switch at site A and the CE switch at site B



NOTE: To purchase a software license for MACsec, contact your Juniper Networks sales representative (<https://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper Networks sales representative will provide you with a feature license file and a license key. You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the `show virtual-chassis` or `show chassis hardware` command.

Overview and Topology

In this example, financially-sensitive company data is often sent between a user at site A and a user at site B. The company wants to ensure that all network traffic traveling from the user at site A to the user at site B is highly secure and cannot be viewed or corrupted by an attacker. The company is using the industry-standard Layer 2 security provided by MACsec, which provides encryption to ensure data cannot be viewed by attackers and integrity checks to ensure transmitted data is not corrupted, to secure all traffic traveling on the CCC through the MPLS cloud connecting the sites. VLANs are configured at both sites to ensure traffic traveling between the two users traverses the sites over the MACsec-secured CCC.

The MPLS network in this example includes two provider edge (PE) switches—PE1 and PE2—and one provider (transit) switch. PE1 connects the customer edge (CE) switch at site A to the MPLS network and PE2 connects the CE switch at site B to the MPLS network. MACsec is enabled on the CCC connecting the CE switches at site A and site B to secure traffic traveling between the sites over the CCC. A VLAN that includes the interfaces that connect the users to the CE switches, interface ge-0/0/0 on the CE switch at site A and interface ge-0/0/2 on the CE switch at site B, and the interfaces that connect the CE switches to the MPLS cloud (ge-0/0/0 on the site A CE switch and xe-0/1/0 on the site B CE switch), is used to direct all traffic between the users onto the MACsec-secured CCC.

Figure 12 on page 283 shows the topology used in this example. The MACsec-secured CCC traffic is labeled **MACsec CCC** in the figure.

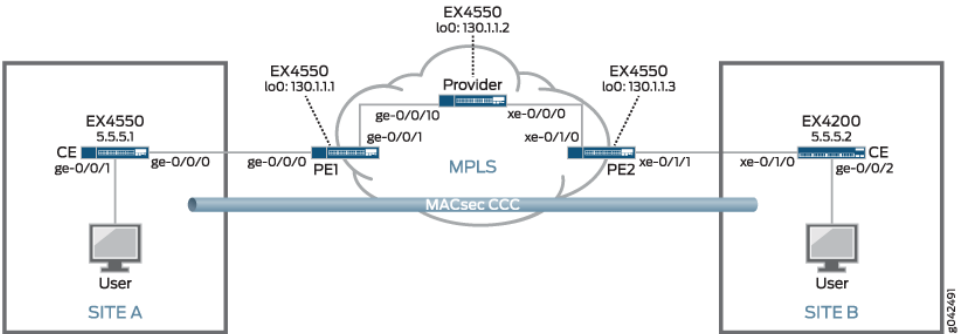


Table 11 on page 284 provides a summary of the MPLS network components in this topology.

Table 12 on page 285 provides a summary of the MACsec connectivity association used in this topology. MACsec is enabled by creating a connectivity association on the interfaces at each end of a link. MACsec is enabled when the interfaces at each end of the link exchange pre-shared keys—the pre-shared keys are defined in the connectivity association—to secure the link for MACsec.

Table 13 on page 285 provides a summary of the VLAN used in this topology. The VLAN is used in this topology to direct all communication from the user at site A to the user at site B onto the MACsec-secured CCC.

Table 11: Components of the MPLS Topology

Component	Description
PE1	<p>PE switch.</p> <p>lo0:</p> <ul style="list-style-type: none"> IP address: 130.1.1.1/32 Participates in OSPF and RSVP. <p>ge-0/0/0:</p> <ul style="list-style-type: none"> Customer edge interface connecting site A to the MPLS network. CCC connecting to xe-0/1/1 on PE2. <p>ge-0/0/1:</p> <ul style="list-style-type: none"> Core interface connecting PE1 to the provider switch. IP address: 10.1.5.2/24 Participates in OSPF, RSVP, and MPLS.
Provider	<p>Provider switch.</p> <p>lo0:</p> <ul style="list-style-type: none"> IP address: 130.1.1.2/32 Participates in OSPF and RSVP. <p>ge-0/0/10:</p> <ul style="list-style-type: none"> Core interface connecting the provider switch to PE1. IP address: 10.1.5.1/24 Participates in OSPF, RSVP, and MPLS. <p>xe-0/0/0:</p> <ul style="list-style-type: none"> Core interface connecting the provider switch to PE2. IP address: 10.1.9.1/24 Participates in OSPF, RSVP, and MPLS.
PE2	<p>PE switch.</p> <p>lo0:</p> <ul style="list-style-type: none"> IP address: 130.1.1.3/32 Participates in OSPF and RSVP. <p>xe-0/1/0</p> <ul style="list-style-type: none"> Core interface connecting PE2 to the provider switch. IP address: 10.1.9.2/24 Participates in OSPF, RSVP, and MPLS. <p>xe-0/1/1</p> <ul style="list-style-type: none"> Customer edge interface connecting site B to the MPLS network. CCC connecting to ge-0/0/0 on PE1.

Table 11: Components of the MPLS Topology (continued)

Component	Description
<code>lsp_to_pe2_xe1</code> label-switched path	Label-switched path from PE1 to PE2.
<code>lsp_to_pe1_ge0</code> label-switched path	Label-switched path from PE2 to PE1.

Table 12: MACsec Connectivity Association Summary

Connectivity Association	Description
<code>ccc-macsec</code>	<p>Connectivity association enabling MACsec on CCC connecting site A to site B.</p> <p>The connectivity association is enabled on the following interfaces:</p> <ul style="list-style-type: none"> Site A CE switch: <code>ge-0/0/0</code> Site B CE switch: <code>xe-0/1/0</code>

Table 13: VLANs Summary

VLAN	Description
<code>macsec</code>	<p>VLAN directing traffic between the user at site A and the user at site B onto the MACsec-secured CCC.</p> <p>The VLAN includes the following interfaces:</p> <ul style="list-style-type: none"> Site A CE switch: <code>ge-0/0/0</code> Site A CE switch: <code>ge-0/0/1</code> Site B CE switch: <code>xe-0/1/0</code> Site B CE switch: <code>ge-0/0/2</code>

Configuring MPLS

This section explains how to configure MPLS on each switch in the MPLS network.

It includes the following sections:

- [Configuring MPLS on Switch PE1 on page 285](#)
- [Configuring MPLS on the Provider Switch on page 288](#)
- [Configuring MPLS on Switch PE2 on page 290](#)
- [Results on page 291](#)

Configuring MPLS on Switch PE1

CLI Quick Configuration

To quickly configure the MPLS configuration on the PE1 switch, use the following commands:

```
[edit]
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ge-0/0/1.0
set protocols mpls label-switched-path lsp_to_pe2_xe1 to 130.1.1.3
```

```
set protocols mpls interface ge-0/0/1.0
set protocols rsvp interface lo0.0
set protocols rsvp interface ge-0/0/1.0
set interfaces lo0 unit 0 family inet address 130.1.1.1/32
set interfaces ge-0/0/1 unit 0 family inet address 10.1.5.2/24
set interfaces ge-0/0/1 unit 0 family mpls
set interfaces ge-0/0/0 unit 0 family ccc
set protocols connections remote-interface-switch ge-1-to-pe2 interface ge-0/0/0.0
set protocols connections remote-interface-switch ge-1-to-pe2 transmit-lsp lsp_to_pe2_xe1
set protocols connections remote-interface-switch ge-1-to-pe2 receive-lsp lsp_to_pe1_ge0
```

Step-by-Step Procedure To configure MPLS on Switch PE1:

1. Configure OSPF with traffic engineering enabled:

```
[edit protocols]
user@switch-PE1# set ospf traffic-engineering
```

2. Configure OSPF on the loopback address and the core interfaces:

```
[edit protocols]
user@switch-PE1# set ospf area 0.0.0.0 interface lo0.0
user@switch-PE1# set ospf area 0.0.0.0 interface ge-0/0/1.0
```

3. Configure MPLS on this switch, PE1, with an LSP to the PE2 switch:

```
[edit protocols]
user@switch-PE1# set mpls label-switched-path lsp_to_pe2_xe1 to 130.1.1.3
```

4. Configure MPLS on the core interfaces:

```
[edit protocols]
user@switch-PE1# set mpls interface ge-0/0/1.0
```

5. Configure RSVP on the loopback interface and the core interfaces:

```
[edit protocols]
user@switch-PE1# set rsvp interface lo0.0
user@switch-PE1# set rsvp interface ge-0/0/1.0
```

6. Configure IP addresses for the loopback interface and the core interfaces:

```
[edit]
user@switch-PE1# set interfaces lo0 unit 0 family inet address 130.1.1.1/32
user@switch-PE1# set interfaces ge-0/0/1 unit 0 family inet address 10.1.5.2/24
```

7. Configure **family mpls** on the logical unit of the core interface addresses:

```
[edit]
user@switch-PE1# set interfaces ge-0/0/1 unit 0 family mpls
```

8. Configure the logical unit of the customer edge interface as a CCC:

```
[edit interfaces ge-0/0/0 unit 0]
user@PE-1# set family ccc
```

9. Configure the interface-based CCC from PE1 to PE2:

```
[edit protocols]
user@PE-1# set connections remote-interface-switch ge-1-to-pe2 interface ge-0/0/0.0
user@PE-1# set connections remote-interface-switch ge-1-to-pe2 transmit-lsp
lsp_to_pe2_xe1
user@PE-1# set connections remote-interface-switch ge-1-to-pe2 receive-lsp lsp_to_pe1_ge0
```

Results Display the results of the configuration:

```
user@PE-1> show configuration
```

```
interfaces {
  ge-0/0/0 {
    unit 0 {
      family ccc;
    }
  }
  ge-0/0/1 {
    unit 0 {
      family inet {
        address 130.1.5.2/24;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 130.1.1.1/32;
      }
    }
  }
}
protocols {
  rsvp {
    interface lo0.0;
    interface ge-0/0/1.0;
  }
  mpls {
    label-switched-path lsp_to_pe2_xe1 {
      to 130.1.1.3;
    }
    interface ge-0/0/1.0;
  }
  ospf {
    traffic-engineering;
    area 0.0.0.0 {
      interface lo0.0;
      interface ge-0/0/1.0;
    }
  }
}
connections {
```

```

remote-interface-switch ge-1-to-pe2 {
  interface ge-0/0/0.0;
  transmit-lsp lsp_to_pe2_xe1;
  receive-lsp lsp_to_pe1_ge0;
}
}
}

```

Configuring MPLS on the Provider Switch

CLI Quick Configuration

To quickly configure the MPLS configuration on the provider switch, use the following commands:

```

[edit]
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ge-0/0/10.0
set protocols ospf area 0.0.0.0 interface xe-0/0/0.0
set protocols mpls interface ge-0/0/10.0
set protocols mpls interface xe-0/0/0.0
set protocols mpls label-switched-path lsp_to_pe2_xe1 to 130.1.1.3
set protocols rsvp interface lo0.0
set protocols rsvp interface ge-0/0/10.0
set protocols rsvp interface xe-0/0/0.0
set interfaces lo0 unit 0 family inet address 130.1.1.2/32
set interfaces ge-0/0/10 unit 0 family inet address 10.1.5.1/24
set interfaces ge-0/0/10 unit 0 family mpls
set interfaces xe-0/0/0 unit 0 family inet address 10.1.9.1/24
set interfaces xe-0/0/0 unit 0 family mpls

```

Step-by-Step Procedure

To configure the provider switch:

1. Configure OSPF with traffic engineering enabled:

```

[edit protocols]
user@switch-P# set ospf traffic-engineering

```

2. Configure OSPF on the loopback interface and the core interfaces:

```

[edit protocols]
user@switch-P# set ospf area 0.0.0.0 interface lo0.0
user@switch-P# set ospf area 0.0.0.0 interface ge-0/0/10.0
user@switch-P# set ospf area 0.0.0.0 interface xe-0/0/0.0

```

3. Configure MPLS on the core interfaces on the switch:

```

[edit protocols]
user@switch-P# set mpls interface ge-0/0/10.0
user@switch-P# set mpls interface xe-0/0/0.0

```

4. Configure RSVP on the loopback interface and the core interfaces:

```

[edit protocols]
user@switch-P# set rsvp interface lo0.0

```

```
user@switch-P# set rsvp interface ge-0/0/10.0
user@switch-P# set rsvp interface xe-0/0/0.0
```

5. Configure IP addresses for the loopback interface and the core interfaces:

```
[edit]
user@switch-P# set interfaces lo0 unit 0 family inet address 130.1.1.2/32
user@switch-P# set interfaces ge-0/0/10 unit 0 family inet address 10.1.5.1/24
user@switch-P# set interfaces xe-0/0/0 unit 0 family inet address 10.1.9.1/24
```

6. Configure **family mpls** on the logical unit of the core interface addresses:

```
[edit]
user@switch-P# set interfaces ge-0/0/10 unit 0 family mpls
user@switch-P# set interfaces xe-0/0/0 unit 0 family mpls
```

7. Configure the LSP to the PE2 switch:

```
[edit]
user@switch-P# set protocols mpls label-switched-path lsp_to_pe2_xe1 to 130.1.1.3
```

Results Display the results of the configuration:

```
user@switch-P> show configuration
```

```
interfaces {
  ge-0/0/10 {
    unit 0 {
      family inet {
        address 10.1.5.1/24;
      }
      family mpls;
    }
  }
  xe-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.9.1/24;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 130.1.1.2/32;
      }
    }
  }
}
protocols {
  rsvp {
    interface lo0.0;
    interface ge-0/0/10.0;
```

```

    interface xe-0/0/0.0;
  }
  mpls {
    label-switched-path lsp_to_pe2_xe1 {
      to 130.1.1.3;
    }
    interface ge-0/0/10.0;
    interface xe-0/0/0.0;
  }
  ospf {
    traffic-engineering;
    area 0.0.0.0 {
      interface lo0.0;
      interface ge-0/0/10.0;
      interface xe-0/0/0.0;
    }
  }
}

```

Configuring MPLS on Switch PE2

CLI Quick Configuration

To quickly cconfigure the MPLS configuration on Switch PE2, use the following commands:

```

[edit]
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface xe-0/1/0.0
set protocols mpls label-switched-path lsp_to_pe1_ge0 to 130.1.1.1
set protocols mpls interface xe-0/1/0.0
set protocols rsvp interface lo0.0
set protocols rsvp interface xe-0/1/0.0
set interfaces lo0 unit 0 family inet address 130.1.1.3/32
set interfaces xe-0/1/0 unit 0 family inet address 10.1.9.2/24
set interfaces xe-0/1/0 unit 0 family mpls
set interfaces xe-0/1/1 unit 0 family ccc
set protocols connections remote-interface-switch xe-1-to-pe1 interface xe-0/1/1.0
set protocols connections remote-interface-switch xe-1-to-pe1 transmit-lsp lsp_to_pe1_ge0
set protocols connections remote-interface-switch xe-1-to-pe1 receive-lsp lsp_to_pe2_xe1

```

Step-by-Step Procedure

To configure Switch PE2:

1. Configure OSPF with traffic engineering enabled:

```

[edit protocols]
user@switch-PE2# set ospf traffic-engineering

```

2. Configure OSPF on the loopback interface and the core interface:

```

[edit protocols]
user@switch-PE2# set ospf area 0.0.0.0 interface lo0.0
user@switch-PE2# set ospf area 0.0.0.0 interface xe-0/1/0.0

```

3. Configure MPLS on this switch (PE2) with a label-switched path (LSP) to the other PE switch (PE1):

```
[edit protocols]
user@switch-PE2# set mpls label-switched-path lsp_to_pe1_ge0 to 130.1.1.1
```

4. Configure MPLS on the core interface:

```
[edit protocols]
user@switch-PE2# set mpls interface xe-0/1/0.0
```

5. Configure RSVP on the loopback interface and the core interface:

```
[edit protocols]
user@switch-PE2# set rsvp interface lo0.0
user@switch-PE2# set rsvp interface xe-0/1/0.0
```

6. Configure IP addresses for the loopback interface and the core interface:

```
[edit]
user@switch-PE2# set interfaces lo0 unit 0 family inet address 130.1.1.3/32
user@switch-PE2# set interfaces xe-0/1/0 unit 0 family inet address 10.1.9.2/24
```

7. Configure **family mpls** on the logical unit of the core interface:

```
[edit]
user@switch-PE2# set interfaces xe-0/1/0 unit 0 family mpls
```

8. Configure the logical unit of the customer edge interface as a CCC:

```
[edit interfaces xe-0/1/1 unit 0]
user@switch-PE2# set family ccc
```

9. Configure the interface-based CCC between the primary edge switches:

```
[edit protocols]
user@switch-PE2# set connections remote-interface-switch xe-1-to-pe1 interface xe-0/1/1.0
user@switch-PE2# set connections remote-interface-switch xe-1-to-pe1 transmit-lsp
lsp_to_pe1_ge0
user@switch-PE2# set connections remote-interface-switch xe-1-to-pe1 receive-lsp
lsp_to_pe2_xe1
```

Results

Display the results of the configuration:

```
user@switch-PE2> show configuration
```

```
interfaces {
  xe-0/1/0 {
    unit 0 {
      family inet {
        address 10.1.9.2/24;
      }
      family mpls;
    }
  }
}
```

```
xe-0/1/1 {
  unit 0 {
    family ccc;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 130.1.1.3/32;
    }
  }
}
}
protocols {
  rsvp {
    interface lo0.0;
    interface xe-0/1/0.0;
  }
  mpls {
    label-switched-path lsp_to_pe1_ge0 {
      to 130.1.1.1;
    }
    interface xe-0/1/0.0;
  }
  ospf {
    traffic-engineering;
    area 0.0.0.0 {
      interface lo0.0;
      interface xe-0/1/0.0;
    }
  }
  connections {
    remote-interface-switch xe-1-to-pe1 {
      interface xe-0/1/1.0;
      transmit-lsp lsp_to_pe1_ge0;
      receive-lsp lsp_to_pe2_xe1;
    }
  }
}
```

Configuring MACsec

This section explains how to configure MACsec on each switch in the topology.

It includes the following sections:

- [Configuring MACsec on the Site A CE Switch to Secure Traffic to Site B on page 293](#)
- [Configuring MACsec on the Site B CE Switch to Secure Traffic to Site A on page 294](#)

Configuring MACsec on the Site A CE Switch to Secure Traffic to Site B

CLI Quick Configuration

```
[edit]
set security macsec connectivity-association ccc-macsec security-mode static-cak
set security macsec connectivity-association ccc-macsec pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
set security macsec connectivity-association ccc-macsec pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
set security macsec interfaces ge-0/0/0 connectivity-association ccc-macsec
```

Step-by-Step Procedure

In this example, the traffic between the users that often exchange financially-sensitive data is sent between the sites on a CCC through the MPLS cloud. MACsec is enabled on the CCC by configuring a MACsec connectivity association on the interfaces on the site A and site B CE switches that connect to the MPLS PE switches. The connectivity associations must have matching connectivity-association names (in this example, **ccc-macsec**), matching CKNs (in this example, **37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311**), and CAKs (in this example, **228ef255aa23ff6729ee664acb66e91f**) in order to establish a MACsec-secure connection.

To enable MACsec on the CCC connecting site A to site B, perform the following procedure on the site A CE switch:

1. Create the connectivity association named **ccc-macsec**, and configure the MACsec security mode as **static-cak**:

```
[edit security macsec]
user@switch-CE-A# set connectivity-association ccc-macsec security-mode static-cak
```

2. Create the pre-shared key by configuring the CKN and CAK:

```
[edit security macsec]
user@switch-CE-A# set connectivity-association ccc-macsec pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@switch-CE-A# set connectivity-association ccc-macsec pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```

3. Assign the connectivity association to the interface connecting to the PE1 switch:

```
[edit security macsec]
user@switch-CE-A# set interfaces ge-0/0/0 connectivity-association ccc-macsec
```

This completes the steps for configuring the connectivity association on one end of the CCC. MACsec is not enabled until a connectivity association with matching pre-shared keys is enabled on the opposite end of a link, which in this case is the interface on the site B CE switch, of the CCC. The process for configuring the connectivity association on the site B CE switch is described in the following section.

Results Display the results of the configuration:

```
user@switch-CE-A> show configuration
```

```
security {
  macsec {
    connectivity-association {
      ccc-macsec {
        pre-shared-key {
          cak "$9$rJ-lWLxNdw24Xxik.PQzreK"; ## SECRET-DATA
          ckn 37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311;
        }
        security-mode {
          static-cak;
        }
      }
    }
    interfaces {
      ge-0/0/0 {
        connectivity-association {
          ccc-macsec;
        }
      }
    }
  }
}
```

Configuring MACsec on the Site B CE Switch to Secure Traffic to Site A

CLI Quick Configuration [edit]
 set security macsec connectivity-association ccc-macsec security-mode static-cak
 set security macsec connectivity-association ccc-macsec pre-shared-key ckn
 37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
 set security macsec connectivity-association ccc-macsec pre-shared-key cak
 228ef255aa23ff6729ee664acb66e91f
 set security macsec interfaces xe-0/1/0 connectivity-association ccc-macsec

Step-by-Step Procedure Traffic travels from site B to site A over the MPLS network using a CCC. MACsec is enabled on the CCC by configuring a MACsec connectivity association on the interfaces on the site A and site B CE switches that connect to the MPLS PE switches. The connectivity associations must have matching connectivity-association names (in this example, **ccc-macsec**), matching CKNs (**37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311**), and matching CAKs (**228ef255aa23ff6729ee664acb66e91f**) in order to establish a MACsec-secure connection.

To enable MACsec on the CCC connecting site B to site A, perform the following procedure on the site B CE switch:

1. Create the connectivity association named **ccc-macsec**, and configure the MACsec security mode as **static-cak**:

```
[edit security macsec]
user@switch-CE-B# set connectivity-association ccc-macsec security-mode static-cak
```

2. Create the pre-shared key by configuring the CKN and CAK:

```
[edit security macsec]
user@switch-CE-B# set connectivity-association ccc-macsec pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@switch-CE-B# set connectivity-association ccc-macsec pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```

3. Assign the connectivity association to the interface connecting to Switch PE2:

```
[edit security macsec]
user@switch-CE-B# set interfaces xe-0/1/0 connectivity-association ccc-macsec
```

MACsec is enabled for the CCC after the pre-shared keys are exchanged, which is shortly after this procedure is completed.

Results Display the results of the configuration:

```
user@switch-CE-B> show configuration
```

```
security {
  macsec {
    connectivity-association {
      ccc-macsec {
        security-mode {
          static-cak;
        }
        pre-shared-key {
          cak "$9$rJ-IWLxNdw24Xxik.PQzreK"; ## SECRET-DATA
          ckn 37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311;
        }
      }
    }
  }
  interfaces {
    xe-0/1/0 {
      connectivity-association {
        ccc-macsec;
      }
    }
  }
}
```

Configuring VLANs to Direct Traffic onto the MACsec-Secured CCC

This section explains how to configure VLANs on the site A and site B CE switches. The purpose of the VLANs is to direct traffic that you want to be MACsec-secured onto the MACsec-secured CCC.

- [Configuring the VLAN to Direct Traffic to the MACsec CCC on the Site A CE Switch on page 296](#)
- [Configuring the VLAN to Direct Traffic to the MACsec CCC on the Site B CE Switch on page 297](#)

Configuring the VLAN to Direct Traffic to the MACsec CCC on the Site A CE Switch

CLI Quick Configuration

```
[edit]
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members macsec
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members macsec
set interfaces vlan unit 50 family inet address 5.5.5.1/24
set vlans macsec vlan-id 50
set vlans macsec l3-interface vlan.50
```

Step-by-Step Procedure

To create a VLAN (VLAN ID 50) that directs traffic from the user at site A onto the MACsec-secured CCC:

1. Configure the ge-0/0/0 interface into the macsec VLAN:

```
[edit interfaces ge-0/0/0 unit 0]
user@switch-CE-A# set family ethernet-switching vlan members macsec
```

2. Configure the ge-0/0/2 interface into the macsec VLAN:

```
[edit interfaces ge-0/0/2 unit 0]
user@switch-CE-A# set family ethernet-switching vlan members macsec
```

3. Create the IP address for the macsec VLAN broadcast domain:

```
[edit interfaces]
user@switch-CE-A# set vlan unit 50 family inet address 5.5.5.1/24
```

4. Configure the VLAN tag ID to 50 for the macsec VLAN:

```
[edit vlans]
user@switch-CE-A# set macsec vlan-id 50
```

5. Associate a Layer 3 interface with the macsec VLAN:

```
[edit vlans]
user@switch-CE-A# set macsec l3-interface vlan.50
```

Results Display the results of the configuration:

```

user@switch-CE-A> show configuration
interfaces {
  ge-0/0/0 {
    unit 0 {
      family ethernet-switching {
        vlan members macsec;
      }
    }
  }
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        vlan members macsec;
      }
    }
  }
  vlan {
    unit 50 {
      family inet address 5.5.5.1/24;
    }
  }
}
vlans {
  macsec {
    l3-interface vlan.50;
    vlan-id 50;
  }
}

```

Configuring the VLAN to Direct Traffic to the MACsec CCC on the Site B CE Switch

CLI Quick Configuration

```

[edit]
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members macsec
set interfaces xe-0/1/0 unit 0 family ethernet-switching vlan members macsec
set interfaces vlan unit 50 family inet address 5.5.5.2/24
set vlans macsec vlan-id 50
set vlans macsec l3-interface vlan.50

```

Step-by-Step Procedure

To create a VLAN (VLAN ID 50) to direct traffic for the user at site B onto the MACsec-secured CCC:

1. Configure the ge-0/0/2 interface into the macsec VLAN:

```

[edit interfaces ge-0/0/2 unit 0]
user@switch-CE-B# set family ethernet-switching vlan members macsec

```

2. Configure the xe-0/1/0 interface into the macsec VLAN:

```

[edit interfaces xe-0/1/0 unit 0]
user@switch-CE-B# set family ethernet-switching vlan members macsec

```

3. Create the IP address for the macsec VLAN broadcast domain:

```
[edit interfaces]
user@switch-CE-B# set vlan unit 50 family inet address 5.5.5.2/24
```

4. Configure the VLAN tag ID to 50 for the macsec VLAN:

```
[edit vlans]
user@switch-CE-B# set macsec vlan-id 50
```

5. Associate a Layer 3 interface with the macsec VLAN:

```
[edit vlans]
user@switch-CE-B# set macsec l3-interface vlan.50
```

Results Display the results of the configuration:

```
user@switch-CE-B> show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        vlan members macsec;
      }
    }
  }
  xe-0/1/0 {
    unit 0 {
      family ethernet-switching {
        vlan members macsec;
      }
    }
  }
  vlan {
    unit 50 {
      family inet address 5.5.5.2/24;
    }
  }
}
vlans {
  macsec {
    l3-interface vlan.50;
    vlan-id 50;
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying the MACsec Connection on page 299](#)
- [Verifying That MACsec-Secured Traffic Is Traversing the CCCs on page 299](#)
- [Verifying That the MPLS and CCC Protocols Are Enabled on the Provider Edge and Provider Switch Interfaces on page 300](#)

- [Verifying MPLS Label Operations on page 301](#)
- [Verifying the Status of the MPLS CCCs on page 302](#)
- [Verifying OSPF Operation on page 303](#)
- [Verifying the Status of the RSVP Sessions on page 303](#)

Verifying the MACsec Connection

Purpose Verify that MACsec is operational on the CCC.

Action Enter the [show security macsec connections](#) command on one or both of the customer edge (CE) switches.

```
user@switch-CE-A> show security macsec connections
Interface name: ge-0/0/0
  CA name: ccc-macsec
  Cipher suite: GCM-AES-128   Encryption: on
  Key server offset: 0         Include SCI: no
  Replay protect: off         Replay window: 0
  Outbound secure channels
    SC Id: 00:19:E2:53:CD:F3/1
    Outgoing packet number: 9785
    Secure associations
      AN: 0 Status: inuse Create time: 2d 20:47:54
  Inbound secure channels
    SC Id: 00:23:9C:0A:53:33/1
    Secure associations
      AN: 0 Status: inuse Create time: 2d 20:47:54
```

Meaning The **Interface name:** and **CA name:** outputs shows that the ccc-macsec connectivity association is operational on interface ge-0/0/0. The output does not appear when the connectivity association is not operational on the interface.

For additional verification that MACsec is operational on the CCC, you can also enter the [show security macsec connections](#) command on the other CE switch.

Verifying That MACsec-Secured Traffic Is Traversing the CCCs

Purpose Verify that traffic traversing the CCC is MACsec-secured.

Action Enter the [show security macsec statistics](#) command on one or both of the CE switches.

```
user@switch-CE-A> show security macsec statistics
Interface name: ge-0/0/0
  Secure Channel transmitted
    Encrypted packets: 9784
    Encrypted bytes: 2821527
    Protected packets: 0
    Protected bytes: 0
  Secure Association transmitted
```

```

Encrypted packets: 9784
Protected packets: 0
Secure Channel received
Accepted packets: 9791
Validated bytes: 0
Decrypted bytes: 2823555
Secure Association received
Accepted packets: 9791
Validated bytes: 0
Decrypted bytes: 2823555

```

Meaning The **Encrypted packets** line under the **Secure Channel transmitted** output is incremented each time a packet is sent from the interface that is secured and encrypted by MACsec. The **Encrypted packets** output shows that 9784 encrypted and secured packets have been transmitted from interface ge-0/0/0. MACsec-secured traffic is, therefore, being sent on interface ge-0/0/0.

The **Accepted packets** line under the **Secure Association received** output is incremented each time a packet that has passed the MACsec integrity check is received on the interface. The **Decrypted bytes** line under the **Secure Association received** output is incremented each time an encrypted packet is received and decrypted. The output shows that 9791 MACsec-secured packets have been received on interface ge-0/0/0, and that 2823555 bytes from those packets have been successfully decrypted. MACsec-secured traffic is, therefore, being received on interface ge-0/0/0.

For additional verification, you can also enter the **show security macsec statistics** command on the other CE switch.

Verifying That the MPLS and CCC Protocols Are Enabled on the Provider Edge and Provider Switch Interfaces

Purpose Verify that MPLS is enabled on the correct interfaces for the PE and provider switches.

Action Enter the **show interfaces terse** command on both of the PE switches and the provider switch:

```
user@switch-PE1> show interfaces terse
```

Interface	Admin	Link	Proto	Local	Remote
ge-0/0/0	up	up			
ge-0/0/0.0	up	up	ccc		
ge-0/0/1	up	up			
ge-0/0/1.0	up	up	inet mpls	10.1.5.2/24	

<some output removed for brevity>

```
user@switch-P> show interfaces terse
```

Interface	Admin	Link	Proto	Local	Remote
xe-0/0/0	up	up			
xe-0/0/0.0	up	up	inet	10.1.9.1/24	


```

                                mpls
ge-0/0/10                      up   up
ge-0/0/10.0                    up   up   inet   10.1.5.1/24
                                mpls
<some output removed for brevity>

```

```
user@switch-PE2> show interfaces terse
```

```

Interface      Admin Link Proto      Local      Remote
xe-0/1/0        up   up
xe-0/1/0.0      up   up   inet      10.1.9.2/24
                                mpls
xe-0/1/1        up   up
xe-0/1/1.0      up   up   ccc
<some output removed for brevity>

```

Meaning The output confirms that the MPLS protocol is up for the provider switch interfaces passing MPLS traffic—xe-0/0/0 and ge-0/0/10—and on the PE switch interfaces passing MPLS traffic, which is interface ge-0/0/1 on the PE1 switch and interface xe-0/1/0 on the PE2 switch.

The output also confirms that CCC is enabled on the PE switch interfaces facing the CE switches, which are interface ge-0/0/0 on the PE1 switch and interface xe-0/1/1 on the PE2 switch.

Verifying MPLS Label Operations

Purpose Verify which interface is being used as the beginning of the CCC and which interface is being used to push the MPLS packet to the next hop.

Action Enter the **show route forwarding-table family mpls** on one or both of the PE switches.

```
user@switch-PE1> show route forwarding-table family mpls
```

```

Routing table: default.mpls
MPLS:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0
0                user  0
1                user  0
2                user  0
13               user  0
299856           user  0
ge-0/0/0.0 (CCC) user  0 10.1.5.1      Push 299952 1328 2 ge-0/0/1.0

```

Meaning This output confirms that the CCC is configured on interface ge-0/0/0.0. The switch receives ingress traffic on ge-0/0/1.0 and pushes label 299952 onto the packet, which exits the switch through interface ge-0/0/1.0. The output also shows that when the

switch receives an MPLS packet with label 299856, it pops the label and sends the packet out through interface ge-0/0/0.0

For further verification of MPLS label operations, enter the **show route forwarding-table family mpls** on the other PE switch.

Verifying the Status of the MPLS CCCs

Purpose Verify that the MPLS CCCs are operating.

Action Enter the **show connections** command on the PE switches.

```
user@switch-PE1> show connections
```

CCC and TCC connections [Link Monitoring On]

Legend for status (St):

UN -- uninitialized
NP -- not present
WE -- wrong encapsulation
DS -- disabled
Dn -- down
-> -- only outbound conn is up
<- -- only inbound conn is up
Up -- operational
RmtDn -- remote CCC down
Restart -- restarting

Legend for connection types:

if-sw: interface switching
rmt-if: remote interface switching
lsp-sw: LSP switching
tx-p2mp-sw: transmit P2MP switching
rx-p2mp-sw: receive P2MP switching

Legend for circuit types:

intf -- interface
oif -- outgoing interface
tlsp -- transmit LSP
rlsp -- receive LSP

Connection/Circuit	Type	St	Time last up	# Up trans
ge-1-to-pe2	rmt-if	Up	May 30 19:01:45	1
ge-0/0/0.0	intf	Up		
lsp_to_pe2_xe1	tlsp	Up		
lsp_to_pe1_ge0	rlsp	Up		

```
user@switch-PE2> show connections
```

CCC and TCC connections [Link Monitoring On]

Legend for status (St):

UN -- uninitialized
NP -- not present
WE -- wrong encapsulation
DS -- disabled
Dn -- down
-> -- only outbound conn is up
<- -- only inbound conn is up
Up -- operational
RmtDn -- remote CCC down
Restart -- restarting

Legend for connection types:

if-sw: interface switching
rmt-if: remote interface switching
lsp-sw: LSP switching
tx-p2mp-sw: transmit P2MP switching
rx-p2mp-sw: receive P2MP switching

Legend for circuit types:

intf -- interface
oif -- outgoing interface
tlsp -- transmit LSP
rlsp -- receive LSP

Connection/Circuit	Type	St	Time last up	# Up trans
xe-1-to-pe1	rmt-if	Up	May 30 09:39:15	1
xe-0/1/1.0	intf	Up		
lsp_to_pe1_ge0	tlsp	Up		
lsp_to_pe2_xe1	rlsp	Up		

The **show connections** command displays the status of the CCC connections. This output verifies that the CCC interfaces and their associated transmit and receive LSPs are **Up** on both PE switches.

Verifying OSPF Operation

Purpose Verify that OSPF is running.

Action Enter the **show ospf neighbor** command on the provider or the PE switches, and check the **State** output.

```
user@switch-P> show ospf neighbor
```

Address	Interface	State	ID	Pri	Dead
10.1.5.2	ge-0/0/10.0	Full	130.1.1.1	128	33
10.1.9.2	xe-0/0/0.0	Full	130.1.1.3	128	38

Meaning The **State** output is **Full** on all interfaces using OSPF, so OSPF is operating.

For further verification on OSPF, enter the **show ospf neighbor** command on the PE switches in addition to the provider switch.

Verifying the Status of the RSVP Sessions

Purpose Verify the status of the RSVP sessions.

Action Enter the **show rsvp session** command, and verify that the state is up for each RSVP session.

```
user@switch-P> show rsvp session
```

```
Ingress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

```
Egress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

```
Transit RSVP: 2 sessions
To          From          State  Rt  Style Labelin Labelout LSPname
130.1.1.1   130.1.1.3       Up     0   1 FF  299936  299856 lsp_to_pe1_ge0
130.1.1.3   130.1.1.1       Up     0   1 FF  299952  299840 lsp_to_pe2_xe1
Total 2 displayed, Up 2, Down 0
```

Meaning The **State** is **Up** for all connections, so RSVP is operating normally.

For further verification, enter the **show rsvp session** on the PE switches in addition to the provider switch.

- Related Documentation**
- [Configuring MACsec on EX, SRX and Fusion Devices on page 228](#)
 - [Understanding Media Access Control Security \(MACsec\) on page 217](#)

Example: Configuring MACsec over an MPLS CCC on MX Series Routers

This example shows how to enable MACsec to secure sensitive traffic traveling from a user at one site to a user at another site over a basic MPLS CCC.

- [Requirements on page 304](#)
- [Overview and Topology on page 304](#)
- [Configuring MPLS on page 307](#)
- [Configuring MACsec on page 314](#)
- [Configuring VLANs to Direct Traffic onto the MACsec-Secured CCC on page 318](#)
- [Verification on page 321](#)

Requirements

This example uses the following hardware and software components:

- Three MX Series routers used as the PE and provider routers in the MPLS network
- One MX Series router used as the CE router connecting site A to the MPLS network
- One MX240, MX480, or MX960 router with the enhanced 20-port Gigabit Ethernet MIC (model number MIC-3D-20GE-SFP-E) used as the CE router connecting site B to the MPLS network
- Junos OS Release 15.1R1 or later running on all MX Series routers in the MPLS network (PE1, PE2, or the provider router)
- Junos OS Release 15.1R1 or later running on the CE router at site A and the CE router at site B

Overview and Topology

In this example, financially-sensitive company data is often sent between a user at site A and a user at site B. The company wants to ensure that all network traffic traveling from the user at site A to the user at site B is highly secure and cannot be viewed or corrupted by an attacker. The company is using the industry-standard Layer 2 security provided by MACsec, which provides encryption to ensure data cannot be viewed by attackers and integrity checks to ensure transmitted data is not corrupted, to secure all traffic traveling on the CCC through the MPLS cloud connecting the sites. VLANs are configured at both sites to ensure traffic traveling between the two users traverses the sites over the MACsec-secured CCC.

The MPLS network in this example includes two provider edge (PE) routers—PE1 and PE2—and one provider (transit) router. PE1 connects the customer edge (CE) router at site A to the MPLS network and PE2 connects the CE router at site B to the MPLS network. MACsec is enabled on the CCC connecting the CE routers at site A and site B to secure

traffic traveling between the sites over the CCC. A VLAN that includes the interfaces that connect the users to the CE routers, interface ge-0/0/0 on the CE router at site A and interface ge-0/0/2 on the CE router at site B, and the interfaces that connect the CE routers to the MPLS cloud (ge-0/0/0 on the site A CE router and xe-0/1/0 on the site B CE router), is used to direct all traffic between the users onto the MACsec-secured CCC.

[Table 11 on page 284](#) provides a summary of the MPLS network components in this topology.

[Table 12 on page 285](#) provides a summary of the MACsec connectivity association used in this topology. MACsec is enabled by creating a connectivity association on the interfaces at each end of a link. MACsec is enabled when the interfaces at each end of the link exchange pre-shared keys—the pre-shared keys are defined in the connectivity association—to secure the link for MACsec.

[Table 13 on page 285](#) provides a summary of the bridge domain and VLAN IDs used in this topology. The VLAN is used in this topology to direct all communication from the user at site A to the user at site B onto the MACsec-secured CCC.

Table 14: Components of the MPLS Topology

Component	Description
PE1	<p>PE router.</p> <p>lo0:</p> <ul style="list-style-type: none"> • IP address: 130.1.1.1/32 • Participates in OSPF and RSVP. <p>ge-0/0/0:</p> <ul style="list-style-type: none"> • Customer edge interface connecting site A to the MPLS network. • CCC connecting to xe-0/1/1 on PE2. <p>ge-0/0/1:</p> <ul style="list-style-type: none"> • Core interface connecting PE1 to the provider router. • IP address: 10.1.5.2/24 • Participates in OSPF, RSVP, and MPLS.

Table 14: Components of the MPLS Topology (continued)

Component	Description
Provider	<p>Provider router.</p> <p>lo0:</p> <ul style="list-style-type: none"> IP address: 130.1.1.2/32 Participates in OSPF and RSVP. <p>ge-0/0/10:</p> <ul style="list-style-type: none"> Core interface connecting the provider router to PE1. IP address: 10.1.5.1/24 Participates in OSPF, RSVP, and MPLS. <p>xe-0/0/0:</p> <ul style="list-style-type: none"> Core interface connecting the provider router to PE2. IP address: 10.1.9.1/24 Participates in OSPF, RSVP, and MPLS.
PE2	<p>PE router.</p> <p>lo0:</p> <ul style="list-style-type: none"> IP address: 130.1.1.3/32 Participates in OSPF and RSVP. <p>xe-0/1/0</p> <ul style="list-style-type: none"> Core interface connecting PE2 to the provider router. IP address: 10.1.9.2/24 Participates in OSPF, RSVP, and MPLS. <p>xe-0/1/1</p> <ul style="list-style-type: none"> Customer edge interface connecting site B to the MPLS network. CCC connecting to ge-0/0/0 on PE1.
lsp_to_pe2_xe1 label-switched path	Label-switched path from PE1 to PE2.
lsp_to_pe1_ge0 label-switched path	Label-switched path from PE2 to PE1.

Table 15: MACsec Connectivity Association Summary

Connectivity Association	Description
ccc-macsec	<p>Connectivity association enabling MACsec on CCC connecting site A to site B.</p> <p>The connectivity association is enabled on the following interfaces:</p> <ul style="list-style-type: none"> Site A CE router: ge-0/0/0 Site B CE router: xe-0/1/0

Table 16: Bridge Domains Summary

Bridge Domain	Description
macsec	<p>VLAN directing traffic between the user at site A and the user at site B onto the MACsec-secured CCC.</p> <p>The bridge domain includes the following interfaces:</p> <ul style="list-style-type: none"> • Site A CE router: ge-0/0/0 • Site A CE router: ge-0/0/1 • Site B CE router: xe-0/1/0 • Site B CE router: ge-0/0/2

Configuring MPLS

This section explains how to configure MPLS on each router in the MPLS network.

It includes the following sections:

- [Configuring MPLS on PE1 on page 307](#)
- [Configuring MPLS on the Provider Router on page 309](#)
- [Configuring MPLS on PE2 on page 312](#)
- [Results on page 313](#)

Configuring MPLS on PE1

CLI Quick Configuration

To quickly configure the MPLS configuration on the PE1 router, use the following commands:

```
[edit]
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ge-0/0/1.0
set protocols mpls label-switched-path lsp_to_pe2_xe1 to 130.1.1.3
set protocols mpls interface ge-0/0/1.0
set protocols rsvp interface lo0.0
set protocols rsvp interface ge-0/0/1.0
set interfaces lo0 unit 0 family inet address 130.1.1.3/32
set interfaces ge-0/0/1 unit 0 family inet address 10.1.5.2/24
set interfaces ge-0/0/1 unit 0 family mpls
set interfaces ge-0/0/0 unit 0 family ccc
set protocols connections remote-interface-switch ge-1-to-pe2 interface ge-0/0/0.0
set protocols connections remote-interface-switch ge-1-to-pe2 transmit-lsp lsp_to_pe2_xe1
set protocols connections remote-interface-switch ge-1-to-pe2 receive-lsp lsp_to_pe1_ge0
```

Step-by-Step Procedure

To configure MPLS on router PE1:

1. Configure OSPF with traffic engineering enabled:

```
[edit protocols]
user@router-PE1# set ospf traffic-engineering
```

2. Configure OSPF on the loopback address and the core interfaces:

```
[edit protocols]
user@router-PE1# set ospf area 0.0.0.0 interface lo0.0
user@router-PE1# set ospf area 0.0.0.0 interface ge-0/0/1.0
```

3. Configure MPLS on this router, PE1, with an LSP to the PE2 router:

```
[edit protocols]
user@router-PE1# set mpls label-switched-path lsp_to_pe2_xe1 to 130.1.1.3
```

4. Configure MPLS on the core interfaces:

```
[edit protocols]
user@router-PE1# set mpls interface ge-0/0/1.0
```

5. Configure RSVP on the loopback interface and the core interfaces:

```
[edit protocols]
user@router-PE1# set rsvp interface lo0.0
user@router-PE1# set rsvp interface ge-0/0/1.0
```

6. Configure IP addresses for the loopback interface and the core interfaces:

```
[edit]
user@router-PE1# set interfaces lo0 unit 0 family inet address 130.1.1/32
user@router-PE1# set interfaces ge-0/0/1 unit 0 family inet address 10.1.5.2/24
```

7. Configure **family mpls** on the logical unit of the core interface addresses:

```
[edit]
user@router-PE1# set interfaces ge-0/0/1 unit 0 family mpls
```

8. Configure the logical unit of the customer edge interface as a CCC:

```
[edit interfaces ge-0/0/0 unit 0]
user@PE-1# set family ccc
```

9. Configure the interface-based CCC from PE1 to PE2:

```
[edit protocols]
user@PE-1# set connections remote-interface-switch ge-1-to-pe2 interface ge-0/0/0.0
user@PE-1# set connections remote-interface-switch ge-1-to-pe2 transmit-lsp
lsp_to_pe2_xe1
user@PE-1# set connections remote-interface-switch ge-1-to-pe2 receive-lsp lsp_to_pe1_ge0
```

Results Display the results of the configuration:

```
user@PE-1> show configuration
```

```
interfaces {
  ge-0/0/0 {
    unit 0 {
      family ccc;
    }
  }
}
```



```

ge-0/0/1{
  unit 0 {
    family inet {
      address 130.1.5.2/24;
    }
    family mpls;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 130.1.1.1/32;
    }
  }
}
}
protocols {
  rsvp {
    interface lo0.0;
    interface ge-0/0/1.0;
  }
  mpls {
    label-switched-path lsp_to_pe2_xe1 {
      to 130.1.1.3;
    }
    interface ge-0/0/1.0;
  }
  ospf {
    traffic-engineering;
    area 0.0.0.0 {
      interface lo0.0;
      interface ge-0/0/1.0;
    }
  }
  connections {
    remote-interface-switch ge-1-to-pe2 {
      interface ge-0/0/0.0;
      transmit-lsp lsp_to_pe2_xe1;
      receive-lsp lsp_to_pe1_ge0;
    }
  }
}
}

```

Configuring MPLS on the Provider Router

CLI Quick Configuration

To quickly configure the MPLS configuration on the provider router, use the following commands:

```

[edit]
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ge-0/0/10.0
set protocols ospf area 0.0.0.0 interface xe-0/0/0.0
set protocols mpls interface ge-0/0/10.0

```

```
set protocols mpls interface xe-0/0/0.0
set protocols mpls label-switched-path lsp_to_pe2_xe1 to 130.1.1.3
set protocols rsvp interface lo0.0
set protocols rsvp interface ge-0/0/10.0
set protocols rsvp interface xe-0/0/0.0
set interfaces lo0 unit 0 family inet address 130.1.1.2/32
set interfaces ge-0/0/10 unit 0 family inet address 10.1.5.1/24
set interfaces ge-0/0/10 unit 0 family mpls
set interfaces xe-0/0/0 unit 0 family inet address 10.1.9.1/24
set interfaces xe-0/0/0 unit 0 family mpls
```

Step-by-Step Procedure

To configure the provider router:

1. Configure OSPF with traffic engineering enabled:

```
[edit protocols]
user@router-P# set ospf traffic-engineering
```

2. Configure OSPF on the loopback interface and the core interfaces:

```
[edit protocols]
user@router-P# set ospf area 0.0.0.0 interface lo0.0
user@router-P# set ospf area 0.0.0.0 interface ge-0/0/10.0
user@router-P# set ospf area 0.0.0.0 interface xe-0/0/0.0
```

3. Configure MPLS on the core interfaces on the router:

```
[edit protocols]
user@router-P# set mpls interface ge-0/0/10.0
user@router-P# set mpls interface xe-0/0/0.0
```

4. Configure RSVP on the loopback interface and the core interfaces:

```
[edit protocols]
user@router-P# set rsvp interface lo0.0
user@router-P# set rsvp interface ge-0/0/10.0
user@router-P# set rsvp interface xe-0/0/0.0
```

5. Configure IP addresses for the loopback interface and the core interfaces:

```
[edit]
user@router-P# set interfaces lo0 unit 0 family inet address 130.1.1.2/32
user@router-P# set interfaces ge-0/0/10 unit 0 family inet address 10.1.5.1/24
user@router-P# set interfaces xe-0/0/0 unit 0 family inet address 10.1.9.1/24
```

6. Configure **family mpls** on the logical unit of the core interface addresses:

```
[edit]
user@router-P# set interfaces ge-0/0/10 unit 0 family mpls
user@router-P# set interfaces xe-0/0/0 unit 0 family mpls
```

7. Configure the LSP to the PE2 router:

```
[edit]
user@router-P# set protocols mpls label-switched-path lsp_to_pe2_xe1 to 130.1.1.3
```

Results Display the results of the configuration:

user@router-P> show configuration

```
interfaces {
  ge-0/0/10 {
    unit 0 {
      family inet {
        address 10.1.5.1/24;
      }
      family mpls;
    }
  }
  xe-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.9.1/24;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 130.1.1.2/32;
      }
    }
  }
}
protocols {
  rsvp {
    interface lo0.0;
    interface ge-0/0/10.0;
    interface xe-0/0/0.0;
  }
  mpls {
    label-switched-path lsp_to_pe2_xe1 {
      to 130.1.1.3;
    }
    interface ge-0/0/10.0;
    interface xe-0/0/0.0;
  }
  ospf {
    traffic-engineering;
    area 0.0.0.0 {
      interface lo0.0;
      interface ge-0/0/10.0;
      interface xe-0/0/0.0;
    }
  }
}
```

Configuring MPLS on PE2

CLI Quick Configuration

To quickly configure the MPLS configuration on router PE2, use the following commands:

```
[edit]
set protocols ospf traffic-engineering
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface xe-0/1/0.0
set protocols mpls label-switched-path lsp_to_pe1_ge0 to 130.1.1.1
set protocols mpls interface xe-0/1/0.0
set protocols rsvp interface lo0.0
set protocols rsvp interface xe-0/1/0.0
set interfaces lo0 unit 0 family inet address 130.1.1.3/32
set interfaces xe-0/1/0 unit 0 family inet address 10.1.9.2/24
set interfaces xe-0/1/0 unit 0 family mpls
set interfaces xe-0/1/1 unit 0 family ccc
set protocols connections remote-interface-switch xe-1-to-pe1 interface xe-0/1/1.0
set protocols connections remote-interface-switch xe-1-to-pe1 transmit-lsp lsp_to_pe1_ge0
set protocols connections remote-interface-switch xe-1-to-pe1 receive-lsp lsp_to_pe2_xe1
```

Step-by-Step Procedure

To configure router PE2:

1. Configure OSPF with traffic engineering enabled:

```
[edit protocols]
user@router-PE2# set ospf traffic-engineering
```

2. Configure OSPF on the loopback interface and the core interface:

```
[edit protocols]
user@router-PE2# set ospf area 0.0.0.0 interface lo0.0
user@router-PE2# set ospf area 0.0.0.0 interface xe-0/1/0.0
```

3. Configure MPLS on this router (PE2) with a label-switched path (LSP) to the other PE router (PE1):

```
[edit protocols]
user@router-PE2# set mpls label-switched-path lsp_to_pe1_ge0 to 130.1.1.1
```

4. Configure MPLS on the core interface:

```
[edit protocols]
user@router-PE2# set mpls interface xe-0/1/0.0
```

5. Configure RSVP on the loopback interface and the core interface:

```
[edit protocols]
user@router-PE2# set rsvp interface lo0.0
user@router-PE2# set rsvp interface xe-0/1/0.0
```

6. Configure IP addresses for the loopback interface and the core interface:

```
[edit]
user@router-PE2# set interfaces lo0 unit 0 family inet address 130.1.1.3/32
user@router-PE2# set interfaces xe-0/1/0 unit 0 family inet address 10.1.9.2/24
```

- Configure **family mpls** on the logical unit of the core interface:

```
[edit]
user@router-PE2# set interfaces xe-0/1/0 unit 0 family mpls
```

- Configure the logical unit of the customer edge interface as a CCC:

```
[edit interfaces xe-0/1/1 unit 0]
user@router-PE2# set family ccc
```

- Configure the interface-based CCC between the primary edge routers:

```
[edit protocols]
user@router-PE2# set connections remote-interface-switch xe-1-to-pe1 interface xe-0/1/1.0
user@router-PE2# set connections remote-interface-switch xe-1-to-pe1 transmit-lsp
lsp_to_pe1_ge0
user@router-PE2# set connections remote-interface-switch xe-1-to-pe1 receive-lsp
lsp_to_pe2_xe1
```

Results

Display the results of the configuration:

```
user@router-PE2> show configuration
```

```
interfaces {
  xe-0/1/0 {
    unit 0 {
      family inet {
        address 10.1.9.2/24;
      }
      family mpls;
    }
  }
  xe-0/1/1 {
    unit 0 {
      family ccc;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 130.1.1.3/32;
      }
    }
  }
}
protocols {
  rsvp {
    interface lo0.0;
    interface xe-0/1/0.0;
  }
  mpls {
    label-switched-path lsp_to_pe1_ge0 {
```

```
        to 130.1.1.1;
    }
    interface xe-0/1/0.0;
}
ospf {
    traffic-engineering;
    area 0.0.0.0 {
        interface lo0.0;
        interface xe-0/1/0.0;
    }
}
connections {
    remote-interface-switch xe-1-to-pe1 {
        interface xe-0/1/1.0;
        transmit-lsp lsp_to_pe1_ge0;
        receive-lsp lsp_to_pe2_xe1;
    }
}
}
```

Configuring MACsec

This section explains how to configure MACsec on each router in the topology.

It includes the following sections:

- [Configuring MACsec on the Site A CE Router to Secure Traffic to Site B on page 315](#)
- [Configuring MACsec on the Site B CE Router to Secure Traffic to Site A on page 316](#)

Configuring MACsec on the Site A CE Router to Secure Traffic to Site B

CLI Quick Configuration

```
[edit]
set security macsec connectivity-association ccc-macsec security-mode static-cak
set security macsec connectivity-association ccc-macsec pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
set security macsec connectivity-association ccc-macsec pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
set security macsec interfaces ge-0/0/0 connectivity-association ccc-macsec
```

Step-by-Step Procedure

In this example, the traffic between the users that often exchange financially-sensitive data is sent between the sites on a CCC through the MPLS cloud. MACsec is enabled on the CCC by configuring a MACsec connectivity association on the interfaces on the site A and site B CE routers that connect to the MPLS PE routers. The connectivity associations must have matching connectivity-association names (in this example, **ccc-macsec**), matching CKNs (in this example, **37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311**), and CAKs (in this example, **228ef255aa23ff6729ee664acb66e91f**) in order to establish a MACsec-secure connection.

To enable MACsec on the CCC connecting site A to site B, perform the following procedure on the site A CE router:

1. Create the connectivity association named **ccc-macsec**, and configure the MACsec security mode as **static-cak**:

```
[edit security macsec]
user@router-CE-A# set connectivity-association ccc-macsec security-mode static-cak
```

2. Create the pre-shared key by configuring the CKN and CAK:

```
[edit security macsec]
user@router-CE-A# set connectivity-association ccc-macsec pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@router-CE-A# set connectivity-association ccc-macsec pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```

3. Assign the connectivity association to the interface connecting to the PE1 router:

```
[edit security macsec]
user@router-CE-A# set interfaces ge-0/0/0 connectivity-association ccc-macsec
```

This completes the steps for configuring the connectivity association on one end of the CCC. MACsec is not enabled until a connectivity association with matching pre-shared keys is enabled on the opposite end of a link, which in this case is the interface on the site B CE router, of the CCC. The process for configuring the connectivity association on the site B CE router is described in the following section.

Results Display the results of the configuration:

```
user@router-CE-A> show configuration
```

```
security {
  macsec {
    connectivity-association {
      ccc-macsec {
        pre-shared-key {
          cak "$9$rJ-lWLxNdw24Xxik.PQzreK"; ## SECRET-DATA
          ckn 37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311;
        }
        security-mode {
          static-cak;
        }
      }
    }
    interfaces {
      ge-0/0/0 {
        connectivity-association {
          ccc-macsec;
        }
      }
    }
  }
}
```

Configuring MACsec on the Site B CE Router to Secure Traffic to Site A

CLI Quick Configuration [edit]
 set security macsec connectivity-association ccc-macsec security-mode static-cak
 set security macsec connectivity-association ccc-macsec pre-shared-key ckn
 37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
 set security macsec connectivity-association ccc-macsec pre-shared-key cak
 228ef255aa23ff6729ee664acb66e91f
 set security macsec interfaces xe-0/1/0 connectivity-association ccc-macsec

Step-by-Step Procedure Traffic travels from site B to site A over the MPLS network using a CCC. MACsec is enabled on the CCC by configuring a MACsec connectivity association on the interfaces on the site A and site B CE routers that connect to the MPLS PE routers. The connectivity associations must have matching connectivity-association names (in this example, **ccc-macsec**), matching CKNs (**37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311**), and matching CAKs (**228ef255aa23ff6729ee664acb66e91f**) in order to establish a MACsec-secure connection.

To enable MACsec on the CCC connecting site B to site A, perform the following procedure on the site B CE router:

1. Create the connectivity association named **ccc-macsec**, and configure the MACsec security mode as **static-cak**:


```
[edit security macsec]
user@router-CE-B# set connectivity-association ccc-macsec security-mode static-cak
```

2. Create the pre-shared key by configuring the CKN and CAK:

```
[edit security macsec]
user@router-CE-B# set connectivity-association ccc-macsec pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@router-CE-B# set connectivity-association ccc-macsec pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```

3. Assign the connectivity association to the interface connecting to router PE2:

```
[edit security macsec]
user@router-CE-B# set interfaces xe-0/1/0 connectivity-association ccc-macsec
```

MACsec is enabled for the CCC after the pre-shared keys are exchanged, which is shortly after this procedure is completed.

Results Display the results of the configuration:

```
user@router-CE-B> show configuration
```

```
security {
  macsec {
    connectivity-association {
      ccc-macsec {
        security-mode {
          static-cak;
        }
        pre-shared-key {
          cak "$9$rJ-IWLxNdw24Xxik.PQzreK"; ## SECRET-DATA
          ckn 37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311;
        }
      }
    }
  }
  interfaces {
    xe-0/1/0 {
      connectivity-association {
        ccc-macsec;
      }
    }
  }
}
```

Configuring VLANs to Direct Traffic onto the MACsec-Secured CCC

This section explains how to configure VLANs on the site A and site B CE routers. The purpose of the VLANs is to direct traffic that you want to be MACsec-secured onto the MACsec-secured CCC.

- [Configuring the Bridge Domain to Direct Traffic to the MACsec CCC on the Site A CE Router on page 318](#)
- [Configuring the Bridge Domain to Direct Traffic to the MACsec CCC on the Site B CE Router on page 320](#)

Configuring the Bridge Domain to Direct Traffic to the MACsec CCC on the Site A CE Router

CLI Quick Configuration

```
[edit]
set interfaces ge-0/0/0 unit 0 encapsulation vlan-bridge
set interfaces ge-0/0/0 unit 0 family bridge
set interfaces ge-0/0/2 unit 0 encapsulation vlan-bridge
set interfaces ge-0/0/2 unit 0 family bridge
set bridge-domains macsec vlan-id 50
set bridge-domains macsec domain-type bridge
set bridge-domains macsec vlan-id all
set bridge-domains macsec interface ge-0/0/0
set bridge-domains macsec interface ge-0/0/2
set interfaces irb vlan-id 50 family inet address 5.5.5.1/24
```

Step-by-Step Procedure

To create a bridge domain (VLAN ID 50) that directs traffic from the user at site A onto the MACsec-secured CCC:

1. Configure the ge-0/0/0 interface with VLAN encapsulation and the bridge family.

```
user@router-CE-A# set interfaces ge-0/0/0 unit 0 encapsulation vlan-bridge
user@router-CE-A# set interfaces ge-0/0/0 unit 0 family bridge vlan-id 50
```

2. Configure the ge-0/0/2 interface with VLAN encapsulation and the bridge family.

```
[edit]
user@router-CE-A# set interfaces ge-0/0/2 unit 0 encapsulation vlan-bridge
user@router-CE-A# set interfaces ge-0/0/2 unit 0 family bridge vlan-id 50
```

3. Define the macsec bridge domain and associate the interfaces, ge-0/0/0 and ge-0/0/2, with the bridge domain.

```
[edit]
user@router-CE-A# set bridge-domains macsec vlan-id 50
user@router-CE-A# set bridge-domains macsec domain-type bridge
user@router-CE-A# set bridge-domains macsec interface ge-0/0/0
user@router-CE-A# set bridge-domains macsec interface ge-0/0/2
```

4. Create the IP address for the macsec bridge domain:

```
[edit]
user@router-CE-A# set interfaces irb vlan-id 50 family inet address 5.5.5.1/24
```

Results Display the results of the configuration:

```
user@router-CE-A> show configuration
interfaces {
  ge-0/0/0 {
    unit 0 {
      encapsulation vlan-bridge;
      family bridge {
        vlan-id 50;
      }
    }
  }
  ge-0/0/2 {
    unit 0 {
      encapsulation vlan-bridge;
      family bridge {
        vlan-id 50;
      }
    }
  }
}
irb {
  vlan-id 50 {
    family inet address 5.5.5.1/24;
  }
}
}
bridge-domains {
  macsec {
    domain-type bridge;
    vlan-id 50;
    interface ge-0/0/0;
    interface ge-0/0/2;
  }
}
```

Configuring the Bridge Domain to Direct Traffic to the MACsec CCC on the Site B CE Router

CLI Quick Configuration

```
[edit]
set interfaces xe-0/1/0 unit 0 encapsulation vlan-bridge
set interfaces xe-0/1/0 unit 0 family bridge
set interfaces ge-0/0/2 unit 0 encapsulation vlan-bridge
set interfaces ge-0/0/2 unit 0 family bridge
set bridge-domains macsec vlan-id 50
set bridge-domains macsec domain-type bridge
set bridge-domains macsec vlan-id all
set bridge-domains macsec interface ge-0/0/2
set bridge-domains macsec interface xe-0/1/0
set interfaces irb vlan-id 50 family inet address 5.5.5.2/24
```

Step-by-Step Procedure

To create a bridge domain (VLAN ID 50) to direct traffic for the user at site B onto the MACsec-secured CCC:

1. Configure the xe-0/1/0 interface with VLAN encapsulation and the bridge family.

```
user@router-CE-A# set interfaces xe-0/1/0 unit 0 encapsulation vlan-bridge
user@router-CE-A# set interfaces xe-0/1/0 unit 0 family bridge vlan-id 50
```

2. Configure the ge-0/0/2 interface with VLAN encapsulation and the bridge family.

```
[edit]
user@router-CE-A#set interfaces ge-0/0/2 unit 0 encapsulation vlan-bridge
user@router-CE-A#set interfaces ge-0/0/2 unit 0 family bridge vlan-id 50
```

3. Define the macsec bridge domain and associate the interfaces, xe-0/1/0 and ge-0/0/2, with the bridge domain.

```
[edit]
user@router-CE-A# set bridge-domains macsec vlan-id 50
user@router-CE-A# set bridge-domains macsec domain-type bridge
user@router-CE-A# set bridge-domains macsec interface xe-0/1/0
user@router-CE-A# set bridge-domains macsec interface ge-0/0/2
```

4. Create the IP address for the macsec bridge domain:

```
[edit]
user@router-CE-A# set interfaces irb vlan-id 50 family inet address 5.5.5.2/24
```

Results Display the results of the configuration:

```
user@router-CE-B> show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      encapsulation vlan-bridge;
      family bridge {
```

```

        vlan-id 50;
    }
}
}
xe-0/1/0 {
    unit 0 {
        encapsulation vlan-bridge;
        family bridge {
            vlan-id 50;
        }
    }
}
irb {
    vlan-id 50 {
        family inet address 5.5.5.2/24;
    }
}
}
bridge-domains {
    macsec {
        domain-type bridge;
        vlan-id 50;
        interface xe-0/1/0;
        interface ge-0/0/2;
    }
}
}

```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying the MACsec Connection on page 321](#)
- [Verifying That MACsec-Secured Traffic Is Traversing the CCCs on page 322](#)
- [Verifying That the MPLS and CCC Protocols Are Enabled on the Provider Edge and Provider Switch Interfaces on page 323](#)
- [Verifying MPLS Label Operations on page 324](#)
- [Verifying the Status of the MPLS CCCs on page 324](#)
- [Verifying OSPF Operation on page 325](#)
- [Verifying the Status of the RSVP Sessions on page 326](#)

Verifying the MACsec Connection

Purpose Verify that MACsec is operational on the CCC.

Action Enter the `show security macsec connections` command on one or both of the customer edge (CE) switches.

```
user@router-CE-A> show security macsec connections
```

```

Interface name: ge-0/0/0
  CA name: ccc-macsec
  Cipher suite: GCM-AES-128   Encryption: on
  Key server offset: 0         Include SCI: no
  Replay protect: off         Replay window: 0
  Outbound secure channels
    SC Id: 00:19:E2:53:CD:F3/1
    Outgoing packet number: 9785
  Secure associations
    AN: 0 Status: inuse Create time: 2d 20:47:54
  Inbound secure channels
    SC Id: 00:23:9C:0A:53:33/1
  Secure associations
    AN: 0 Status: inuse Create time: 2d 20:47:54

```

Meaning The **Interface name:** and **CA name:** outputs shows that the ccc-macsec connectivity association is operational on interface ge-0/0/0. The output does not appear when the connectivity association is not operational on the interface.

For additional verification that MACsec is operational on the CCC, you can also enter the **show security macsec connections** command on the other CE switch.

Verifying That MACsec-Secured Traffic Is Traversing the CCCs

Purpose Verify that traffic traversing the CCC is MACsec-secured.

Action Enter the **show security macsec statistics** command on one or both of the CE switches.

```
user@router-CE-A> show security macsec statistics
```

```

Interface name: ge-0/0/0
  Secure Channel transmitted
    Encrypted packets: 9784
    Encrypted bytes:   2821527
    Protected packets: 0
    Protected bytes:   0
  Secure Association transmitted
    Encrypted packets: 9784
    Protected packets: 0
  Secure Channel received
    Accepted packets: 9791
    Validated bytes:  0
    Decrypted bytes:  2823555
  Secure Association received
    Accepted packets: 9791
    Validated bytes:  0
    Decrypted bytes:  2823555

```

Meaning The **Encrypted packets** line under the **Secure Channel transmitted** output is incremented each time a packet is sent from the interface that is secured and encrypted by MACsec. The **Encrypted packets** output shows that 9784 encrypted and secured packets have

been transmitted from interface ge-0/0/0. MACsec-secured traffic is, therefore, being sent on interface ge-0/0/0.

The **Accepted packets** line under the **Secure Association received** output is incremented each time a packet that has passed the MACsec integrity check is received on the interface. The **Decrypted bytes** line under the **Secure Association received** output is incremented each time an encrypted packet is received and decrypted. The output shows that 9791 MACsec-secured packets have been received on interface ge-0/0/0, and that 2823555 bytes from those packets have been successfully decrypted. MACsec-secured traffic is, therefore, being received on interface ge-0/0/0.

For additional verification, you can also enter the **show security macsec statistics** command on the other CE switch.

Verifying That the MPLS and CCC Protocols Are Enabled on the Provider Edge and Provider Switch Interfaces

Purpose Verify that MPLS is enabled on the correct interfaces for the PE and provider switches.

Action Enter the **show interfaces terse** command on both of the PE routers and the provider switch:

```
user@router-PE1> show interfaces terse
```

Interface	Admin	Link	Proto	Local	Remote
ge-0/0/0	up	up			
ge-0/0/0.0	up	up	ccc		
ge-0/0/1	up	up			
ge-0/0/1.0	up	up	inet mpls	10.1.5.2/24	

<some output removed for brevity>

```
user@router-P> show interfaces terse
```

Interface	Admin	Link	Proto	Local	Remote
xe-0/0/0	up	up			
xe-0/0/0.0	up	up	inet mpls	10.1.9.1/24	
ge-0/0/10	up	up			
ge-0/0/10.0	up	up	inet mpls	10.1.5.1/24	

<some output removed for brevity>

```
user@router-PE2> show interfaces terse
```

Interface	Admin	Link	Proto	Local	Remote
xe-0/1/0	up	up			
xe-0/1/0.0	up	up	inet mpls	10.1.9.2/24	
xe-0/1/1	up	up			
xe-0/1/1.0	up	up	ccc		

<some output removed for brevity>

Meaning The output confirms that the MPLS protocol is up for the provider switch interfaces passing MPLS traffic—xe-0/0/0 and ge-0/0/10—and on the PE router interfaces passing MPLS traffic, which is interface ge-0/0/1 on the PE1 switch and interface xe-0/1/0 on the PE2 router.

The output also confirms that CCC is enabled on the PE router interfaces facing the CE switches, which are interface ge-0/0/0 on the PE1 switch and interface xe-0/1/1 on the PE2 router.

Verifying MPLS Label Operations

Purpose Verify which interface is being used as the beginning of the CCC and which interface is being used to push the MPLS packet to the next hop.

Action Enter the **show route forwarding-table family mpls** on one or both of the PE routers.

```
user@router-PE1> show route forwarding-table family mpls
```

```
Routing table: default.mpls
MPLS:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0
0                user  0                recv  49   4
1                user  0                recv  49   4
2                user  0                recv  49   4
13               user  0                recv  49   4
299856           user  0                Pop   1327  2 ge-0/0/0.0
ge-0/0/0.0 (CCC) user  0 10.1.5.1          Push 299952 1328 2 ge-0/0/1.0
```

Meaning This output confirms that the CCC is configured on interface ge-0/0/0.0. The switch receives ingress traffic on ge-0/0/1.0 and pushes label 299952 onto the packet, which exits the switch through interface ge-0/0/1.0. The output also shows that when the switch receives an MPLS packet with label 299856, it pops the label and sends the packet out through interface ge-0/0/0.0

For further verification of MPLS label operations, enter the **show route forwarding-table family mpls** on the other PE router.

Verifying the Status of the MPLS CCCs

Purpose Verify that the MPLS CCCs are operating.

Action Enter the **show connections** command on the PE routers.

```
user@router-PE1> show connections
```

```
CCC and TCC connections [Link Monitoring On]
Legend for status (St):          Legend for connection types:
UN -- uninitialized             if-sw: interface switching
```



```

NP -- not present
WE -- wrong encapsulation
DS -- disabled
Dn -- down
-> -- only outbound conn is up
<- -- only inbound conn is up
Up -- operational
RmtDn -- remote CCC down
Restart -- restarting

rmt-if: remote interface switching
lsp-sw: LSP switching
tx-p2mp-sw: transmit P2MP switching
rx-p2mp-sw: receive P2MP switching
Legend for circuit types:
intf -- interface
oif -- outgoing interface
tlsp -- transmit LSP
rlsp -- receive LSP

```

Connection/Circuit	Type	St	Time last up	# Up trans
ge-1-to-pe2	rmt-if	Up	May 30 19:01:45	1
ge-0/0/0.0	intf	Up		
lsp_to_pe2_xe1	tlsp	Up		
lsp_to_pe1_ge0	rlsp	Up		

```
user@router-PE2> show connections
```

```

CCC and TCC connections [Link Monitoring On]
Legend for status (St):
UN -- uninitialized
NP -- not present
WE -- wrong encapsulation
DS -- disabled
Dn -- down
-> -- only outbound conn is up
<- -- only inbound conn is up
Up -- operational
RmtDn -- remote CCC down
Restart -- restarting

Legend for connection types:
if-sw: interface switching
rmt-if: remote interface switching
lsp-sw: LSP switching
tx-p2mp-sw: transmit P2MP switching
rx-p2mp-sw: receive P2MP switching
Legend for circuit types:
intf -- interface
oif -- outgoing interface
tlsp -- transmit LSP
rlsp -- receive LSP

```

Connection/Circuit	Type	St	Time last up	# Up trans
xe-1-to-pe1	rmt-if	Up	May 30 09:39:15	1
xe-0/1/1.0	intf	Up		
lsp_to_pe1_ge0	tlsp	Up		
lsp_to_pe2_xe1	rlsp	Up		

The **show connections** command displays the status of the CCC connections. This output verifies that the CCC interfaces and their associated transmit and receive LSPs are **Up** on both PE routers.

Verifying OSPF Operation

Purpose Verify that OSPF is running.

Action Enter the **show ospf neighbor** command the provider or the PE routers, and check the **State** output.

```
user@router-P> show ospf neighbor
```

Address	Interface	State	ID	Pri	Dead
10.1.5.2	ge-0/0/10.0	Full	130.1.1.1	128	33
10.1.9.2	xe-0/0/0.0	Full	130.1.1.3	128	38

Meaning The **State** output is **Full** on all interfaces using OSPF, so OSPF is operating.

For further verification on OSPF, enter the **show ospf neighbor** command on the PE routers in addition to the provider switch.

Verifying the Status of the RSVP Sessions

Purpose Verify the status of the RSVP sessions.

Action Enter the **show rsvp session** command, and verify that the state is up for each RSVP session.

```
user@router-P> show rsvp session
```

```
Ingress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Egress RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0

Transit RSVP: 2 sessions
To          From          State  Rt  Style  Labelin  Labelout  LSPname
130.1.1.1   130.1.1.3   Up     0   1 FF   299936   299856   lsp_to_pe1_ge0
130.1.1.3   130.1.1.1   Up     0   1 FF   299952   299840   lsp_to_pe2_xe1
Total 2 displayed, Up 2, Down 0
```

Meaning The **State** is **Up** for all connections, so RSVP is operating normally.

For further verification, enter the **show rsvp session** on the PE routers in addition to the provider router.

PART 5

MAC Limiting and Move Limiting

- [MAC Limiting and Move Limiting Configurations and Examples on page 329](#)

CHAPTER 13

MAC Limiting and Move Limiting Configurations and Examples

- [Understanding MAC Limiting and MAC Move Limiting on page 330](#)
- [Understanding MAC Limiting on Layer 3 Routing Interfaces on page 332](#)
- [Understanding and Using Persistent MAC Learning on page 335](#)
- [Configuring MAC Limiting on page 339](#)
- [Example: Configuring MAC Limiting on page 347](#)
- [Verifying That MAC Limiting Is Working Correctly on page 357](#)
- [Override a MAC Limit Applied to All Interfaces on page 364](#)
- [Configuring MAC Move Limiting \(ELS\) on page 365](#)
- [Verifying That MAC Move Limiting Is Working Correctly on page 366](#)
- [Verifying That the Port Error Disable Setting Is Working Correctly on page 367](#)

Understanding MAC Limiting and MAC Move Limiting

MAC limiting protects against flooding of the Ethernet switching table, and is enabled on Layer 2 interfaces (ports). MAC move limiting detects MAC movement and MAC spoofing on access interfaces. It is enabled on VLANs.

- *MAC limiting* enhances port security by limiting the number of MAC addresses that can be learned within a VLAN. Limiting the number of MAC addresses protects the switch from flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). Flooding occurs when the number of new MAC addresses that are learned causes the Ethernet switching table to overflow, and previously learned MAC addresses are flushed from the table. The switch then reverts to flooding the previously-learned MAC addresses, which can impact performance and introduce security vulnerabilities.
- *MAC move limiting* provides additional security by controlling the number of MAC address moves that are allowed in a VLAN within one second. A MAC address move occurs when the switch receives a packet with a source MAC address that has already been learned by the switch, but on a different interface. The Ethernet switching table is then updated to reflect the association of the MAC address with the new interface. Because the Ethernet switching table must be updated for each MAC address move, frequent move events can lead to exhaustion of the switch's processing resources. This might occur as the result of a MAC spoofing attack or a loop in the network.
- [MAC Limiting on page 330](#)
- [MAC Move Limiting on page 331](#)
- [Actions for MAC Limiting and MAC Move Limiting on page 331](#)

MAC Limiting

With MAC limiting, you limit the MAC addresses that can be learned on Layer 2 access interfaces by either limiting the number of MAC addresses or by specifying allowed MAC addresses:

- Limiting the number of MAC addresses—You configure the maximum number of MAC addresses that can be dynamically learned (added to the Ethernet switching table) per interface. You can specify that incoming packets with new MAC addresses be ignored, dropped, or logged when the limit is exceeded. You can also specify that the interface be shut down or temporarily disabled.



NOTE: Static MAC addresses do not count toward the limit you specify for dynamic MAC addresses.

- Specifying allowed MAC addresses—You configure the allowed MAC addresses for an interface. Any MAC address that is not in the list of configured addresses is not learned, and the switch logs an appropriate message. An allowed MAC address is bound to a VLAN so that the address is not registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.

MAC limiting is configured on Layer 2 interfaces. You can specify the maximum number of dynamic MAC addresses that can be learned on a single interface, all interfaces, or a specific interface on the basis of its membership within a VLAN (VLAN membership MAC limit).

When you are configuring the maximum MAC limit for an interface, you can choose the action that occurs on incoming packets when the MAC limit is exceeded. You can specify that incoming packets be ignored, dropped, or logged when the limit is exceeded. You can also specify that the interface be shut down or temporarily disabled.

MAC limiting is not enabled by default. For additional information about configuring MAC limit for an interface on a device that supports ELS, see *Configuring MAC Limiting (ELS)*. For additional information about configuring MAC limit for an interface on a device that does not support Enhanced Layer 2 Software (ELS), see [“Configuring MAC Limiting \(non-ELS\)” on page 341](#).

See *Using the Enhanced Layer 2 Software CLI* for additional information on ELS.

MAC Move Limiting

With MAC move limiting, you limit the number of times a MAC address can move to a new interface within one second. When MAC move limiting is configured, MAC address movements are tracked by the switch. The first time a MAC address moves is always considered a good move and will not count toward the configured MAC move limit. Monitoring of MAC address moves comes into effect after the first move, even if the MAC move limit is configured as 1.

You configure MAC move limiting on a per-VLAN basis. Although you enable this feature on VLANs, the MAC move limit applies to the number of movements for each individual MAC address rather than the total number of MAC address moves in the VLAN. For example, if the MAC move limit is set to 1, the switch allows an unlimited number of MAC address movements within the VLAN as long as the same MAC address does not move more than once within a second.

You can configure an action to be taken if the MAC address move limit is exceeded. You can specify that incoming packets be ignored, dropped, or logged when the limit is exceeded. You can also specify that the interface be shut down or temporarily disabled.

MAC move limiting is not enabled by default. For additional information about configuring MAC move limiting on a device that does not support ELS, see *Configuring MAC Move Limiting (non-ELS)*. For additional information about configuring MAC move limiting on a device that supports ELS, see [“Configuring MAC Move Limiting \(ELS\)” on page 365](#).

Actions for MAC Limiting and MAC Move Limiting

You can choose to have one of the following actions performed when the MAC limit or the MAC move limit is exceeded:

- **drop**—Drop the packet, but do not generate an alarm.
- **drop-and-log**—Drop the packet and generate an alarm, an SNMP trap, or system log entry.

- **log**—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- **none**—Forward packets with new source MAC addresses, and learn the new source MAC address.
- **shutdown**—Disable the interface in the VLAN and generate an alarm, an SNMP trap, or a system log entry.
- **vlan-member-shutdown**—(EX9200 only) Starting in Junos OS Release 15.1 for MAC Limiting and MAC Move Limiting on EX9200 Switches, the **vlan-member-shutdown** statement is supported to block an interface on the basis of its membership in a specific VLAN and generate an alarm, an SNMP trap, or a system log entry.

In the event of shutdown, you can configure the switch to automatically restore the disabled interfaces to service after a specified period of time. To configure autorecovery on a device that supports ELS, see [“Configuring Autorecovery for Port Security Events” on page 635](#). To configure autorecovery on a device that does not support ELS, see [“Configuring Autorecovery for Port Security Events” on page 635](#).



NOTE: If you do not configure the switch for autorecovery from the disabled condition, you can bring up the disabled interfaces by running one of the following commands:

- (For devices that support ELS)—[clear ethernet-switching recovery-timeout](#)
- (For devices that do not support ELS)—[clear ethernet-switching port-error](#)

Release History Table

Release	Description
15.1	Starting in Junos OS Release 15.1 for MAC Limiting and MAC Move Limiting on EX9200 Switches, the vlan-member-shutdown statement is supported to block an interface on the basis of its membership in a specific VLAN and generate an alarm, an SNMP trap, or a system log entry.

Related Documentation

- [Port Security Features on page 3](#)
- [Configuring MAC Limiting \(ELS\)](#)
- [Configuring Autorecovery for Port Security Events on page 635](#)
- [Adding a Static MAC Address Entry to the Ethernet Switching Table on a Switch with ELS Support](#)

Understanding MAC Limiting on Layer 3 Routing Interfaces

- [Overview on page 333](#)
- [Limitations on page 334](#)

Overview

The MAC limiting feature provides a mechanism for limiting MAC addresses on devices that are connected to a Layer 3 routed Gigabit Ethernet (GE), Fast Ethernet (FE), or 10 Gigabit Ethernet (XE) interface. With MAC filters, you can allow traffic with specific source MAC. Software-based MAC limiting is supported. MAC limiting is applicable only on interfaces with plain Ethernet or VLAN tagged encapsulation.

Both the physical interface level **source-address-filter** and logical interface level **accept-source-mac** configurations are supported on SRX100, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, and SRX650 devices. (Platform support depends on the Junos OS release in your installation.) The following considerations apply when you configure the **source-address-filter** and **accept-source-mac** statements:

- If only the logical level **accept-source-mac** statement is configured, traffic from only those configured MAC addresses will be allowed on the logical interface.
- If only the physical interface level **source-address-filter** statement is configured, the physical interface's *allowed* MAC addresses are also considered the *allowed* addresses for all the logical interfaces belonging to the physical interface. Incoming packets from any other source MAC addresses are dropped.
- If the physical interface level **source-address-filter** is configured under **gigether-options** (or **fastether-options**) and **accept-source-mac** is configured for one or more of its logical interfaces or VLANs, the allowed list of addresses is a combination of MAC addresses specified in both the statements. For logical interfaces and VLANs where the **accept-source-mac** statement is not configured, the physical interface's *allowed* list of addresses is considered.

You can configure an interface to receive packets from specific MAC addresses. To do this, specify the MAC addresses in the **source-address-filter** or **accept-source-mac** statements:

- Logical level MAC filter configuration on an untagged interface

```
ge-0/0/10 {
  unit 0 {
    accept-source-mac {
      mac-address 00:22:33:44:55:66;
      mac-address 00:26:88:e9:a3:01;
    }
    family inet {
      address 60.60.60.1/24;
    }
  }
}
```

- Physical level MAC filter configuration on an untagged interface

```
ge-0/0/10 {
  gigether-options {
    source-address-filter {
```

```

        00:55:55:55:55:66;
        00:26:88:e9:a3:01;
    }
}
unit 0 {
    family inet {
        address 60.60.60.1/24;
    }
}
}

```

- Physical and logical level MAC filter configurations on a tagged interface

```

ge-0/0/10 {
    vlan-tagging;
    gigether-options {
        source-address-filter {
            00:26:88:e9:a3:01;
        }
    }
    unit 0 {
        vlan-id 40;
        accept-source-mac {
            mac-address 00:22:33:44:55:66;
        }
        family inet {
            address 40.40.40.1/24;
        }
    }
    unit 1 {
        vlan-id 60;
        accept-source-mac {
            mac-address 00:55:55:55:55:66;
        }
        family inet {
            address 60.60.60.1/24;
        }
    }
}
}

```



NOTE: On untagged Gigabit Ethernet interfaces, you must not configure the `source-address-filter` and the `accept-source-mac` statements simultaneously. If these statements are configured for the same interfaces at the same time, an error message appears. However, in the case of tagged VLANs, both these statements can be configured simultaneously, if no identical MAC addresses are specified.

Limitations

The following limitations apply to MAC limiting support on Layer 3 routed GE, FE, or XE interfaces:

- You can configure only 32 MAC addresses per device.
- Only software-based MAC filtering is supported. Software-based MAC filtering impacts performance. The performance impact is proportional to the number of MAC addresses configured.
- MAC- based policer or rate limiting is not supported.
- You cannot configure broadcast or multicast address in the source-address-filter statement.
- MAC filtering is not supported on Aggregated Ethernet (AE), Fabric Ethernet, Point-to-Point Protocol over Ethernet (PPPoE), Routed VLAN interface (RVI), or VLAN interfaces.

MAC filtering is not supported on chassis clusters.

Related Documentation

- *Understanding Interface Logical Properties*

Understanding and Using Persistent MAC Learning

- [Understanding Persistent MAC Learning \(Sticky MAC\) on page 335](#)
- [Configuring Persistent MAC Learning \(ELS\) on page 337](#)
- [Configuring Persistent MAC Learning \(non-ELS\) on page 338](#)
- [Verifying That Persistent MAC Learning Is Working Correctly on page 339](#)

Understanding Persistent MAC Learning (Sticky MAC)

Persistent MAC learning, also known as sticky MAC, is a port security feature that enables an interface to retain dynamically learned MAC addresses when the switch is restarted or if the interface goes down and is brought back online.

Persistent MAC address learning is disabled by default. You can enable persistent MAC address learning in conjunction with MAC limiting to restrict the number of persistent MAC addresses. You enable this feature on interfaces.

Configure persistent MAC learning on an interface to:

- Prevent traffic losses for trusted workstations and servers because the interface does not have to relearn the addresses from ingress traffic after a restart.
- Protect the switch against security attacks. Use persistent MAC learning in combination with MAC limiting to protect against attacks, such as Layer 2 denial-of-service (DoS) attacks, overflow attacks on the Ethernet switching table, and DHCP starvation attacks, by limiting the MAC addresses allowed while still allowing the interface to dynamically learn a specified number of MAC addresses. The interface is secured because after the limit has been reached, additional devices cannot connect to the port.

By configuring persistent MAC learning along with MAC limiting, you enable interfaces to learn MAC addresses of trusted workstations and servers from the time when you connect the interface to your network until the limit for MAC addresses is reached, and

ensure that after this limit is reached, new devices will not be allowed to connect to the interface even if the switch restarts. As an alternative to using persistent MAC learning with MAC limiting, you can statically configure each MAC address on each port or allow the port to continuously learn new MAC addresses after restarts or interface-down events. Allowing the port to continuously learn MAC addresses represents a security risk.



NOTE: While a switch is restarting or an interface is coming back up, there might be a short delay before the interface can learn more MAC addresses. This delay occurs while the system re-enters previously learned persistent MAC addresses into the forwarding database for the interface.

Consider the following configuration guidelines when configuring persistent MAC learning:

- Interfaces must be configured in access mode (use the **port-mode** configuration statement or, for switches operating on the Enhanced Layer 2 Software (ELS) configuration style, the **interface-mode** configuration statement).
- You cannot enable persistent MAC learning on an interface on which 802.1x authentication is configured.
- You cannot enable persistent MAC learning on an interface that is part of a redundant trunk group.
- You cannot enable persistent MAC learning on an interface on which **no-mac-learning** is enabled.



TIP: If you move a device within your network that has a persistent MAC address entry on the switch, use the **clear ethernet-switching table** command to clear the persistent MAC address entry from the interface. If you move the device and do not clear the persistent MAC address from the original port it was learned on, then the new port will not learn the MAC address of the device and the device will not be able to connect. If the original port is down when you move the device, then the new port will learn the MAC address and the device can connect. However, if you do not clear the persistent MAC address on the original port, then when the port restarts, the system reinstalls the persistent MAC address in the forwarding table for that port. If this occurs, the persistent MAC address is removed from the new port and the device loses connectivity.

Configuring Persistent MAC Learning (ELS)



NOTE: This section describes using Junos OS with support for the Enhanced Layer 2 Software (ELS). For more information on ELS, see *Using the Enhanced Layer 2 Software CLI*

To configure persistent MAC learning on an interface and limit the number of allowed MAC addresses:

1. Enable persistent MAC learning on an interface:

```
[edit switch-options]
user@switch# set interface interface-name persistent-learning
```

2. Configure the MAC limit on an interface, and specify the action that the switch takes after the specified limit is exceeded:

```
[edit switch-options]
user@switch# set interface interface-name interface-mac-limit limit packet-action action
```

After you set a new MAC limit for the interface, the system clears existing entries in the MAC address forwarding table associated with the interface.

Values for *action* are:

drop—Drop packets with new source MAC addresses, and do not learn the new source MAC addresses.

drop-and-log—(EX Series switches only) Drop packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

log—(EX Series switches only) Hold packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

none—(EX Series switches only) Forward packets with new source MAC addresses, and learn the new source MAC address.

shutdown—(EX Series switches only) Disable the specified interface, and generate an alarm, an SNMP trap, or a system log entry.



TIP: If you move a device within your network that has a persistent MAC address entry on the switch, use the `clear ethernet-switching table` command to clear the persistent MAC address entry from the interface. If you move the device and do not clear the persistent MAC address from the original port it was learned on, then the new port will not learn the MAC address of the device and the device will not be able to connect.

If the original port is down when you move the device, then the new port will learn the MAC address and the device can connect. However, if you do not

clear the persistent MAC address on the original port, then when the port restarts, the system reinstalls the persistent MAC address in the forwarding table for that port. If this occurs, the persistent MAC address is removed from the new port and the device loses connectivity.

Configuring Persistent MAC Learning (non-ELS)

Persistent MAC address learning, also known as sticky MAC, is disabled by default. You can enable it to allow dynamically learned MAC addresses to be retained on an interface across restarts of the switch.



NOTE: This section describes using Junos OS without support for the Enhanced Layer 2 Software (ELS). For more information on ELS, see *Using the Enhanced Layer 2 Software CLI*

Use persistent MAC address learning to:

- Help prevent traffic losses for trusted workstations and servers because the interface does not have to relearn the addresses from ingress traffic after a restart.
- Protect the switch against security attacks—use persistent MAC learning in combination with MAC limiting to protect against attacks while still avoiding the need to statically configure MAC addresses. When the initial learning of MAC addresses up to the number specified by the MAC limit is done, new addresses will not be allowed even after a reboot. The port is secured because after the limit has been reached, additional devices cannot connect to the interface.

The first devices that send traffic after you connect are learned during the initial connection period. You can monitor the MAC addresses and provide the same level of security as if you statically configured each MAC address on each interface, except with less manual effort. Persistent MAC learning also helps prevent traffic loss for trusted workstations and servers because the interface does not have to relearn the addresses from ingress traffic.

To configure persistent MAC learning on an interface and limit the number of allowed MAC addresses:

1. Enable persistent MAC learning on an interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name persistent-learning
```

2. Configure the MAC limit on an interface, and specify the action that the switch takes after the specified limit is exceeded:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name mac-limit limit packet-action action
```

After you set a new MAC limit for the interface, the system clears existing entries in the MAC address forwarding table associated with the interface.

Verifying That Persistent MAC Learning Is Working Correctly

Purpose Verify that persistent MAC learning, also known as sticky MAC, is working on the interface. Persistent MAC learning allows retention of dynamically learned MAC addresses on an interface across restarts of the switch (or if the interface goes down).

Action Display the MAC addresses that have been learned. The following sample output shows the results when persistent MAC learning is enabled on interface ge-0/0/42:

show ethernet-switching table persistent-mac

```
user@switch> show ethernet-switching table
```

```
Ethernet-switching table: 8 entries, 2 learned, 5 persistent entries
VLAN      MAC address      Type      Age      Interfaces
default   *                Flood     -        All-members
default   00:10:94:00:00:02 Persistent      0 ge-0/0/42.0
default   00:10:94:00:00:03 Persistent      0 ge-0/0/42.0
default   00:10:94:00:00:04 Persistent      0 ge-0/0/42.0
default   00:10:94:00:00:05 Persistent      0 ge-0/0/42.0
default   00:10:94:00:00:06 Persistent      0 ge-0/0/42.0
default   00:21:59:c8:0c:50 Learn          0 ae0.0
default   02:21:59:c8:0c:44 Learn          0 ae0.0
```

Meaning The sample output shows that learned MAC addresses are stored in the Ethernet switching table as persistent entries. If the switch is rebooted or the interface goes down and comes back up, these addresses will be restored to the table.

See Also

- [Configuring Port Security \(non-ELS\) on page 11](#)
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)

Configuring MAC Limiting

- [Configuring MAC Limiting \(ELS\) on page 339](#)
- [Configuring MAC Limiting \(non-ELS\) on page 341](#)
- [Configuring MAC Limiting \(QFX Switches\) on page 344](#)
- [Configuring MAC Limiting \(J-Web Procedure\) on page 346](#)

Configuring MAC Limiting (ELS)

This topic describes different ways of configuring a limitation on MAC addresses in packets that are received and forwarded by the switch.



NOTE: The tasks presented in the first section uses Junos OS for EX Series switches and QFX3500 and QFX3600 switches with support for the Enhanced Layer 2 Software (ELS) configuration style. See *Using the Enhanced Layer 2 Software CLI* for more information about ELS configurations.

- For information on configuring an interface to automatically recover from a shutdown caused by MAC limiting, see [“Configuring Autorecovery for Port Security Events” on page 635](#). If you do not configure the switch for autorecovery from the disabled condition, you can bring up the disabled interfaces by running the `clear ethernet-switching recovery-timeout` command.

The different ways of setting a MAC limit are described in the following sections:

- [Limiting the Number of MAC Addresses Learned by an Interface on page 340](#)
- [Limiting the Number of MAC Addresses Learned by a VLAN on page 340](#)

Limiting the Number of MAC Addresses Learned by an Interface

To secure a port, you can set the maximum number of MAC addresses that can be learned by an interface:

- Set the MAC limit on an interface, and specify an action that the switch takes after the specified limit is exceeded:

```
[edit switch-options]
user@switch# set interface interface-name interface-mac-limit limit packet-action
action
```

After you set a new MAC limit for the interface, the system clears existing entries in the MAC address forwarding table associated with the interface.

Limiting the Number of MAC Addresses Learned by a VLAN

To limit the number of MAC addresses learned by a VLAN, perform both of the following steps:

1. Set the maximum number of MAC addresses that can be learned by a VLAN, and specify an action that the switch takes after the specified limit is exceeded:

```
[edit vlans]
user@switch# set vlan-name switch-options mac-table-size limit packet-action
action
```

2. Set the maximum number of MAC addresses that can be learned by one *or* all interfaces in the VLAN, and specify an action that the switch takes after the specified limit is exceeded:



NOTE: If you specify a MAC limit and packet action for all interfaces in the VLAN *and* a specific interface in the VLAN, the MAC limit and packet action specified at the specific interface level takes precedence. Also, at the VLAN interface level, only the drop and drop-and-log options are supported.

```
[edit vlans]
user@switch# set vlan-name switch-options interface interface-name
interface-mac-limit limit packet-action action

[edit vlans]
user@switch# set vlan-name switch-options interface-mac-limit limit packet-action
action
```

After you set new MAC limits for a VLAN by using the **mac-table-size** statement or for interfaces associated with a VLAN by using the **interface-mac-limit** statement, the system clears the corresponding existing entries in the MAC address forwarding table.



NOTE: On a QFX Series Virtual Chassis, if you include the shutdown option at the [edit vlans *vlan-name* switch-options interface *interface-name* interface-mac-limit packet-action] hierarchy level and issue the commit operation, the system generates a commit error. The system does not generate an error if you include the shutdown option at the [edit switch-options interface *interface-name* interface-mac-limit packet-action] hierarchy level.

Configuring MAC Limiting (non-ELS)

This task uses Junos OS for EX Series switches and QFX3500 and QFX3600 switches that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Configuring MAC Limiting (ELS)*. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

This topic describes various ways of configuring a limitation on MAC addresses in packets that are received and forwarded by the switch.

Before you can change a MAC limit that was previously set for an interface or a VLAN, you must first clear existing entries in the MAC address forwarding table that correspond to the change you want to make. Thus, to change the limit on an interface, first clear the MAC address forwarding table entries for that interface. To change the limit on all interfaces and VLANs, clear all MAC address forwarding table entries. To change the limit on a VLAN, clear the MAC address forwarding table entries for that VLAN.

To clear MAC addresses from the forwarding table:

- Clear MAC address entries from a specific interface (here, the interface is **ge-0/0/1**) in the forwarding table:

```
user@switch> clear ethernet-switching-table interface ge-0/0/1
```

- Clear all MAC address entries in the forwarding table:

```
user@switch>clear ethernet-switching-table
```

- Clear MAC address entries from a specific VLAN (here, the VLAN is vlan-abc):

```
user@switch> clear ethernet-switching-table vlan vlan-abc
```

The different ways of setting a MAC limit are described in the following sections:

- [Limiting the Number of MAC Addresses That Can be Learned on Interfaces on page 342](#)
- [Specifying MAC Addresses That Are Allowed on page 342](#)
- [Configuring MAC Limiting for VLANs on page 343](#)

Limiting the Number of MAC Addresses That Can be Learned on Interfaces

To configure MAC limiting for port security by setting a maximum number of MAC addresses that can be learned on interfaces.

- Apply the MAC limit on a single interface (here, the interface is ge-0/0/1):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 mac-limit 10
```

When no action is specified for configuring the MAC limit on an interface, the switch performs the default action **drop** if the limit is exceeded.

- Apply the MAC limit on a single access interface, on the basis of its membership within a specific VLAN (here, the interface is ge-0/0/1 and the VLAN is vl.

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 vlan vl mac-limit 5
```

With this type of configuration, the switch drops any additional packets if the limit is exceeded, and also logs a message.

- Apply the limit to all access interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all mac-limit 10
```

When no action is specified for configuring the MAC limit on all interfaces, the switch performs the default action **drop** if the limit is exceeded:

Specifying MAC Addresses That Are Allowed

You must clear existing entries in the MAC address forwarding table prior to changing the MAC address limit.

To configure MAC limiting for port security by specifying allowed MAC addresses:

- On a single interface (here, the interface is ge-0/0/2):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
```

- On all interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch#set interface all allowed-mac 00:05:85:3A:82:80
user@switch#set interface all allowed-mac 00:05:85:3A:82:81
user@switch#set interface all allowed-mac 00:05:85:3A:82:83
```

Configuring MAC Limiting for VLANs

You must clear existing entries in the MAC address forwarding table before you can change the MAC address limit.

MAC limiting for a VLAN restricts the MAC addresses that can be learned for that VLAN, but does *not* drop the packet. Therefore, setting the MAC limit on a VLAN is not considered a port-security feature.



NOTE: The configuration of specific allowed MAC addresses does not apply to VLANs.

To configure MAC limiting for a VLAN using the CLI:

- Limit the number of dynamic MAC addresses on a VLAN:

If the MAC limit on a specific VLAN is exceeded, the switch logs the MAC addresses of packets that cause the limit to be exceeded. No other action is possible.

```
[edit vlans]
user@switch# set vlan-abc mac-limit 20
```



NOTE: When you are applying a MAC limit on a VLAN, do not set `mac-limit` to 1 for a VLAN composed of Routed VLAN Interfaces (RVIs) or a VLAN composed of aggregated Ethernet bundles using LACP. In these cases, setting the `mac-limit` to 1 prevents the switch from learning MAC addresses other than the automatic addresses:

- For RVIs, the first MAC address inserted into the forwarding database is the MAC address of the RVI.
- For aggregated Ethernet bundles using LACP, the first MAC address inserted into the forwarding database in the forwarding table is the source address of the protocol packet.

If the VLAN is composed of regular access or trunk interfaces, you can set the `mac-limit` to 1 if you choose to do so.

- See Also**
- [Example: Protecting against Ethernet Switching Table Overflow Attacks on page 354](#)
 - [Verifying That MAC Limiting Is Working Correctly on page 357](#)
 - [Override a MAC Limit Applied to All Interfaces on page 364](#)
 - [Configuring Autorecovery for Port Security Events on page 635](#)
 - [Understanding MAC Limiting and MAC Move Limiting for Port Security](#)
 - [Understanding Bridging and VLANs on Switches](#)

Configuring MAC Limiting (QFX Switches)

To configure MAC limiting on a specific interface or on all interfaces:

1. To limit the number of dynamic MAC addresses, set a MAC limit of 5.

The action is not specified, so the switch performs the default action **drop** if the limit is exceeded:

- On a single interface (here, the interface is `xe-0/0/1`):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface xe-0/0/1 mac-limit (Access Port Security) 5
```

- On all interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all mac-limit 5
```



CAUTION: Do not set the MAC limit to 1. The first learned MAC address is often inserted into the forwarding database automatically. (For instance, the first MAC address inserted into the forwarding database for routed VLAN interfaces is the MAC address of the RVI. For Aggregated Ethernet bundles using LACP, the first MAC address inserted into the forwarding database in the forwarding table is the source address of the protocol packet.) The switch therefore fails to learn MAC addresses other than the automatic addresses when the MAC limit is set to 1, and this causes problems with MAC learning and forwarding.

2. To specify allowed MAC addresses:

- On a single interface (here, the interface is `xe-0/0/2`):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface xe-0/0/2 allowed-mac 00:05:85:3A:82:80
user@switch# set interface xe-0/0/2 allowed-mac 00:05:85:3A:82:81
user@switch# set interface xe-0/0/2 allowed-mac 00:05:85:3A:82:83
```

- On all interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all allowed-mac 00:05:85:3A:82:80
user@switch# set interface all allowed-mac 00:05:85:3A:82:81
user@switch# set interface all allowed-mac 00:05:85:3A:82:83
```

- See Also**
- [Port Security Features on page 3](#)
 - [Understanding MAC Limiting and MAC Move Limiting for Port Security](#)
 - [Understanding How to Protect Access Ports from Common Attacks on page 6](#)
 - [Verifying That MAC Limiting Is Working Correctly on page 357](#)
 - [Example: Protecting against Ethernet Switching Table Overflow Attacks on page 354](#)
 - [Example: Protecting against DHCP Starvation Attacks on page 347](#)
 - `no-allowed-mac-log`

Configuring MAC Limiting (J-Web Procedure)

MAC limiting protects against flooding of the Ethernet switching table on an EX Series switch. MAC limiting sets a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface (port).

Junos OS provides two MAC limiting methods:

- Maximum number of dynamic MAC addresses allowed per interface—If the limit is exceeded, incoming packets with new MAC addresses are dropped.
- Specific “allowed” MAC addresses for the access interface—Any MAC address that is not in the list of configured addresses is not learned.

You configure MAC limiting for each interface, not for each VLAN. You can specify the maximum number of dynamic MAC addresses that can be learned on a single Layer 2 access interface or on all Layer 2 access interfaces. The default action that the switch will take if that maximum number is exceeded is **drop**—drop the packet and generate an alarm, an SNMP trap, or a system log entry.

To enable MAC limiting on one or more interfaces using the J-Web interface:

1. Select **Configure>Security>Port Security**.
2. Select one or more interfaces from the **Interface List**.
3. Click the **Edit** button. If a message appears asking whether you want to enable port security, click **Yes**.
4. To set a dynamic MAC limit:
 1. Type a limit value in the **MAC Limit** box.
 2. Select an action from the **MAC Limit Action** box (optional). The switch takes this action when the MAC limit is exceeded. If you do not select an action, the switch applies the default action, **drop**.
 - Log—Generate a system log entry.
 - Drop—Drop the packets and generate a system log entry. (Default)
 - Shutdown—Shut down the VLAN and generate a system log entry. You can mitigate the effect of this option by configuring the switch for autorecovery from the disabled state and specifying a **disable timeout** value.
 - None— No action to be taken.
5. To add allowed MAC addresses:
 1. Click **Add**.
 2. Type the allowed MAC address and click **OK**.Repeat this step to add more allowed MAC addresses.

6. Click **OK** when you have finished setting MAC limits.
7. Click **OK** after the configuration has been successfully delivered.



NOTE: You can enable or disable port security on the switch at any time by clicking the **Activate** or **Deactivate** button on the Port Security Configuration page. If security status is shown as **Disabled** when you try to edit settings for any VLANs or interfaces (ports), a message asking whether you want to enable port security appears.

- See Also**
- [Example: Protecting against DHCP Starvation Attacks on page 347](#)
 - [Verifying That MAC Limiting Is Working Correctly on page 357](#)
 - [Understanding MAC Limiting and MAC Move Limiting on page 330](#)

Example: Configuring MAC Limiting

- [Example: Protecting against DHCP Starvation Attacks on page 347](#)
- [Example: Protecting against Rogue DHCP Server Attacks on page 351](#)
- [Example: Protecting against Ethernet Switching Table Overflow Attacks on page 354](#)

Example: Protecting against DHCP Starvation Attacks

In a DHCP starvation attack, an attacker floods an Ethernet LAN with DHCP requests from spoofed (counterfeit) MAC addresses, causing the switch's overworked DHCP server to stop assigning IP addresses and lease times to legitimate DHCP clients on the switch (hence the name starvation). Requests from those clients are either dropped or directed to a rogue DHCP server set up by the attacker.

This example describes how to configure MAC limiting, a port security feature, to protect the switch against DHCP starvation attacks:

- [Requirements on page 347](#)
- [Overview and Topology on page 348](#)
- [Configuration on page 349](#)
- [Verification on page 350](#)

Requirements

This example uses the following hardware and software components:

- One EX Series or QFX3500 switch
- Junos OS Release 9.0 or later for EX Series switches, or Junos OS Release 12.1 or later for the QFX Series switch
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure MAC limiting, a port security feature, to mitigate DHCP starvation attacks, be sure you have:

- Connected the DHCP server to the switch.
- Configured the VLAN **employee-vlan** on the switch.

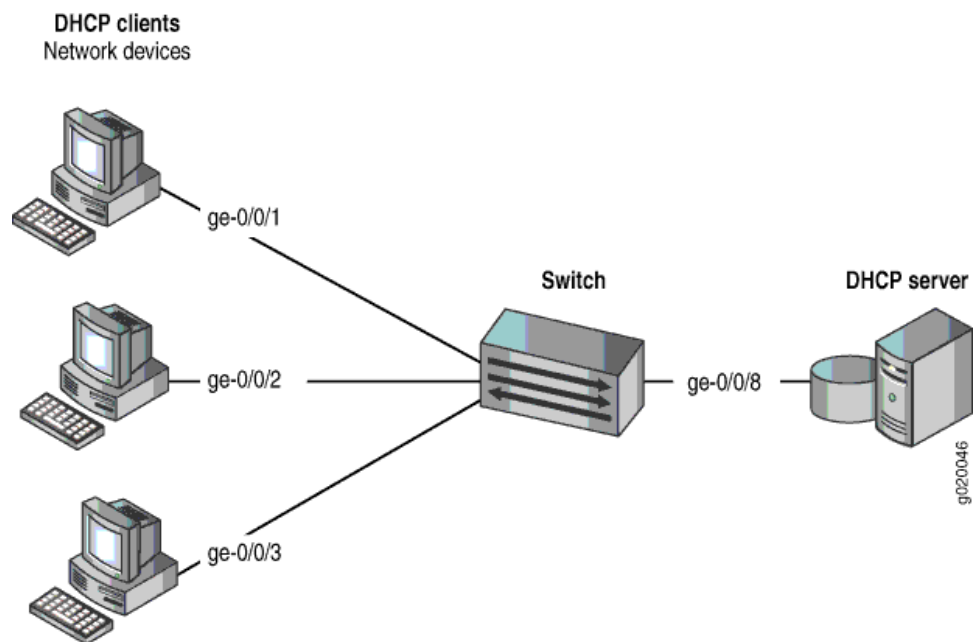
Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch against one common type of attack, a DHCP starvation attack.

This example shows how to configure port security features on a switch connected to a DHCP server. The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN on an EX Series switch is described in the topic, *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*. The procedure is not repeated here.

Figure 13 on page 348 illustrates the topology for this example.

Figure 13: Network Topology for Basic Port Security



The components of the topology for this example are shown in Table 17 on page 348.

Table 17: Components of the Port Security Topology

Properties	Settings
Switch hardware	QFX3500 switch
VLAN name and ID	employee-vlan

Table 17: Components of the Port Security Topology (continued)

Properties	Settings
Interfaces in employee-vlan	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface for DHCP server	ge-0/0/8

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- No MAC limit is set on any of the interfaces.
- DHCP snooping is disabled on the VLAN **employee-vlan**.
- All access interfaces are untrusted, which is the default setting.

Configuration

To configure the MAC limiting port security feature to protect the switch against DHCP starvation attacks:

- [\[xref target has no title\]](#)

CLI Quick Configuration

To quickly configure MAC limiting, copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/1 mac-limit 3 action drop
set interface ge-0/0/2 mac-limit 3 action drop
```

Step-by-Step Procedure

Configure MAC limiting:

1. Configure a MAC limit of **3** on **ge-0/0/1** and specify that packets with new addresses be dropped if the limit has been exceeded on the interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 mac-limit 3 action drop
```

2. Configure a MAC limit of **3** on **ge-0/0/2** and specify that packets with new addresses be dropped if the limit has been exceeded on the interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/2 mac-limit 3 action drop
```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/1.0 {
  mac-limit 3 action drop;
```

```

}
interface ge-0/0/2.0 {
  mac-limit 3 action drop;
}

```

Verification

To confirm that the configuration is working properly:

- [Verifying That MAC Limiting Is Working Correctly on the Switch on page 350](#)

Verifying That MAC Limiting Is Working Correctly on the Switch

Purpose Verify that MAC limiting is working on the switch.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the MAC addresses learned when DHCP requests are sent from hosts on **ge-0/0/1** and from hosts on **ge-0/0/2**, with both interfaces set to a MAC limit of **3** with the action **drop**:

```
user@switch> show vlans
```

Ethernet-switching table: 7 entries, 6 learned

VLAN	MAC address	Type	Age	Interfaces
default	*	Flood	-	ge-0/0/2.0
default	00:05:85:3A:82:77	Learn	0	ge-0/0/1.0
default	00:05:85:3A:82:79	Learn	0	ge-0/0/1.0
default	00:05:85:3A:82:80	Learn	0	ge-0/0/1.0
default	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
default	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
default	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0

Meaning The sample output shows that with a MAC limit of **3** for each interface, the DHCP request for a fourth MAC address on **ge-0/0/2** was dropped because it exceeded the MAC limit.

Because only 3 MAC addresses can be learned on each of the two interfaces, attempted DHCP starvation attacks will fail.

See Also

- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Configuring MAC Limiting \(non-ELS\) on page 341](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security](#)

Example: Protecting against Rogue DHCP Server Attacks

In a rogue DHCP server attack, an attacker has introduced a rogue server into the network, allowing it to give IP address leases to the network's DHCP clients and to assign itself as the gateway device.

This example describes how to configure a DHCP server interface as untrusted to protect the switch from a rogue DHCP server:

- [Requirements on page 351](#)
- [Overview and Topology on page 351](#)
- [Configuration on page 352](#)
- [Verification on page 353](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch or one QFX3500 switch
- Junos OS Release 9.0 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure an untrusted DHCP server interface to mitigate rogue DHCP server attacks, be sure you have:

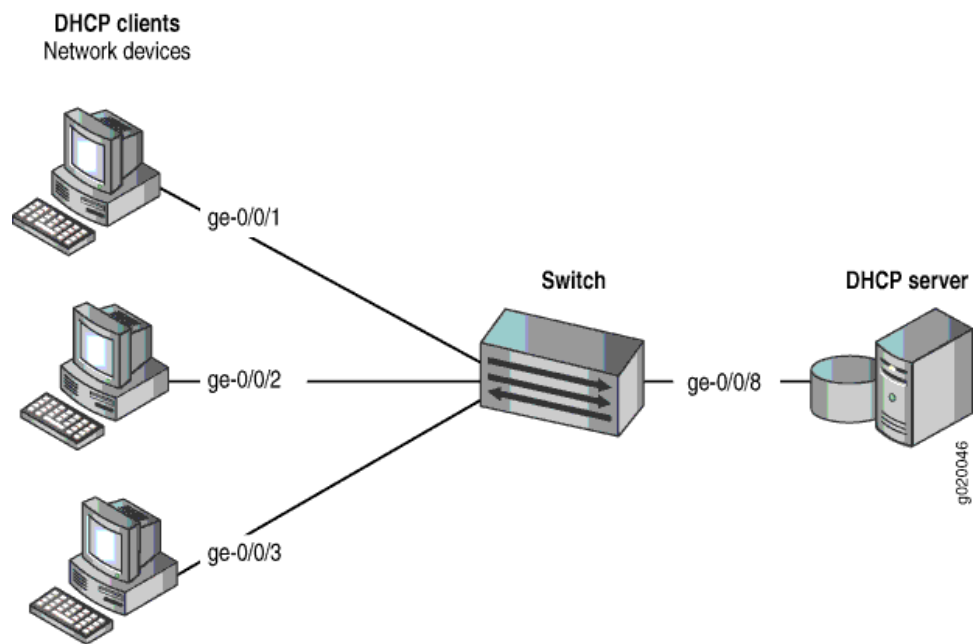
- Connected the DHCP server to the switch.
- Enabled DHCP snooping on the VLAN.
- Configured a VLAN on the switch. See the task for your platform:
 - *Example: Setting Up Bridging with Multiple VLANs.*

Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch from rogue DHCP server attacks.

This example shows how to explicitly configure an untrusted interface on an EX3200-24P switch and a QFX3500 switch. [Figure 14 on page 352](#) illustrates the topology for this example.

Figure 14: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 18 on page 352](#).

Table 18: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	employee-vlan , tag 20
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is the subnet's broadcast address
Interfaces in employee-vlan	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface for DHCP server	ge-0/0/8

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- DHCP snooping is enabled on the VLAN **employee-vlan**.
- The interface (port) where the rogue DHCP server has connected to the switch is currently trusted.

Configuration

To configure the DHCP server interface as untrusted because the interface is being used by a rogue DHCP server:

CLI Quick Configuration To quickly set the rogue DHCP server interface as untrusted, copy the following command and paste it into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/8 no-dhcp-trusted
```

Step-by-Step Procedure To set the DHCP server interface as untrusted:

- Specify the interface (port) from which DHCP responses are not allowed:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/8 no-dhcp-trusted
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/8.0 {
  no-dhcp-trusted;
}
```

Verification

Confirm that the configuration is working properly.

Verifying That the DHCP Server Interface Is Untrusted

Purpose Verify that the DHCP server is untrusted.

- Action**
1. Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.
 2. Display the DHCP snooping information when the port on which the DHCP server connects to the switch is not trusted.

Meaning There is no output from the command because no entries are added to the DHCP snooping database.

- See Also**
- [Understanding and Using Trusted DHCP Servers on page 371](#)
 - [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [show dhcp snooping binding on page 1178](#)

Example: Protecting against Ethernet Switching Table Overflow Attacks

In an Ethernet switching table overflow attack, an intruder sends so many requests from new MAC addresses that the Ethernet switching table fills up and then overflows, forcing the switch to broadcast all messages.

This example describes how to configure MAC limiting and allowed MAC addresses, two port security features, to protect the switch from Ethernet switching table attacks:

- [Requirements on page 354](#)
- [Overview and Topology on page 354](#)
- [Configuration on page 356](#)
- [Verification on page 357](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch or QFX3500 switch
- Junos OS Release 9.0 or later for EX Series switches or Junos OS 12.1 or later for the QFX Series.
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure specific port security features to mitigate common access-interface attacks, be sure you have:

- Connected the DHCP server to the switch.
- Configured a VLAN on the switch. See the task for your platform:

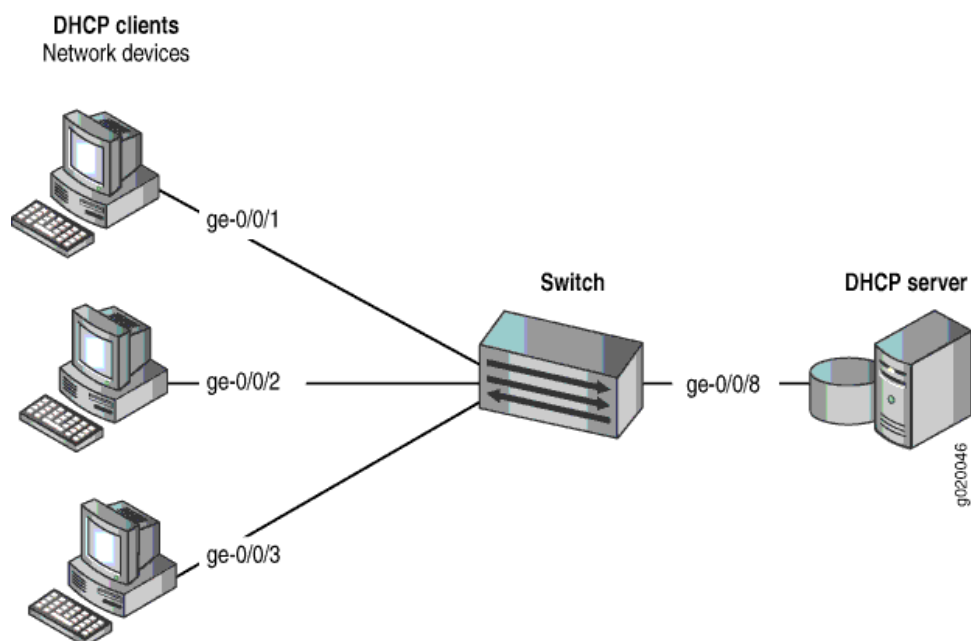
Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch from an attack on the Ethernet switching table that causes the table to overflow and thus forces the switch to broadcast all messages.

This example shows how to configure port security features on a switch connected to a DHCP server.

The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches* and *Example: Setting Up Bridging with Multiple VLANs for the QFX Series*. That procedure is not repeated here. [Figure 15 on page 355](#) illustrates the topology for this example.

Figure 15: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 19 on page 355](#).

Table 19: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX Series switch or one QFX3500 switch
VLAN name and ID	employee-vlan , tag 20
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is subnet's broadcast address
Interfaces in employee-vlan	ge-0/0/1 , ge-0/0/2 , ge-0/0/3 , ge-0/0/8
Interface for DHCP server	ge-0/0/8

In this example, use the MAC limit feature to control the total number of MAC addresses that can be added to the Ethernet switching table for the specified interface. Use the allowed MAC addresses feature to ensure that the addresses of network devices whose network access is critical are guaranteed to be included in the Ethernet switching table.

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- No MAC limit is set on any of the interfaces.
- All access interfaces are untrusted, which is the default setting.

Configuration

To configure MAC limiting and some allowed MAC addresses to protect the switch against Ethernet switching table overflow attacks:

CLI Quick Configuration

To quickly configure MAC limiting, clear the MAC forwarding table, and configure some allowed MAC addresses, copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/1 mac-limit 4 action drop
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
exit
exit
clear ethernet-switching-table interface ge-0/0/1
```

Step-by-Step Procedure

Configure MAC limiting and some allowed MAC addresses:

1. Configure a MAC limit of 4 on **ge-0/0/1** and specify that incoming packets with different addresses be dropped once the limit is exceeded on the interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/1 mac-limit (Access Port Security) 4 action drop
```

2. Clear the current entries for interface **ge-0/0/1** from the MAC address forwarding table :

```
user@switch# clear ethernet-switching-table interface ge-0/0/1
```

3. Configure the allowed MAC addresses on **ge-0/0/2**:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/1.0 {
  mac-limit 4 action drop;
}
interface ge-0/0/2.0 {
  allowed-mac [ 00:05:85:3a:82:80 00:05:85:3a:82:81 00:05:85:3a:82:83 00:05:85:3a:82:85 ];
}
```


Verification

To confirm that the configuration is working properly:

- [Verifying That MAC Limiting Is Working Correctly on the Switch on page 357](#)

Verifying That MAC Limiting Is Working Correctly on the Switch

Purpose Verify that MAC limiting is working on the switch.

Action Display the MAC cache information after DHCP requests have been sent from hosts on **ge-0/0/1**, with the interface set to a MAC limit of 4 with the action **drop**, and after four allowed MAC addresses have been configured on interface **ge-0/0/2**:

```
user@switch> show vlans
```

Ethernet-switching table: 5 entries, 4 learned

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	00:05:85:3A:82:71	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:74	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:77	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:79	Learn	0	ge-0/0/1.0
employee-vlan	*	Flood	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

Meaning The sample output shows that with a MAC limit of 4 for the interface, the DHCP request for a fifth MAC address on **ge-0/0/1** was dropped because it exceeded the MAC limit and that only the specified allowed MAC addresses have been learned on the **ge-0/0/2** interface.

See Also

- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Configuring MAC Limiting \(non-ELS\) on page 341](#)
- [Configuring MAC Move Limiting \(non-ELS\)](#)

Verifying That MAC Limiting Is Working Correctly

MAC limiting protects against flooding of the Ethernet switching table by setting a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface (port)..

Junos OS provides two methods for MAC limiting for port security:

- **Maximum number of MAC addresses**—You configure the maximum number of dynamic MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses can be ignored, dropped, or logged. You can also specify that the interface be shut down or temporarily disabled.
- **Allowed MAC addresses**—You configure specific “allowed” MAC addresses for the access interface. Any MAC address that is not in the list of configured addresses is not learned, and the switch logs an appropriate message. The allowed MAC method binds MAC addresses to a VLAN so that the address is not registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.

Junos OS also allows you to set a MAC limit on VLANs. However, setting a MAC limit on VLANs is not considered a port security feature, because the switch does not prevent incoming packets that cause the MAC limit to be exceeded from being forwarded; it only logs the MAC addresses of these packets.

To verify MAC limiting configurations:

1. [Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly on page 358](#)
2. [Verifying That MAC Limiting for a Specific Interface Within a Specific VLAN Is Working Correctly on page 359](#)
3. [Verifying That Allowed MAC Addresses Are Working Correctly on page 360](#)
4. [Verifying Results of Various Action Settings When the MAC Limit Is Exceeded on page 361](#)
5. [Verifying That Interfaces Are Shut Down on page 363](#)
6. [Customizing the Ethernet Switching Table Display to View Information for a Specific Interface on page 363](#)

Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly

Purpose Verify that MAC limiting for dynamic MAC addresses is working on the switch.

Action Display the MAC addresses that have been learned. The following sample output shows the results when two packets were sent from hosts on ge-0/0/1 and five packets requests were sent from hosts on ge-0/0/2, with both interfaces set to a MAC limit of 4 with the default action **drop**:

```
user@switch> show ethernet-switching table
```

```
Ethernet-switching table: 7 entries, 6 learned
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	-	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:77	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:79	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0

Meaning The sample output shows that with a MAC limit of 4 for each interface, the packet for a fifth MAC address on ge-0/0/2 was dropped because it exceeded the MAC limit. The address was not learned, and thus an asterisk (*) rather than an address appears in the **MAC address** column in the first line of the sample output.

Verifying That MAC Limiting for a Specific Interface Within a Specific VLAN Is Working Correctly

Purpose Verify that MAC limiting for a specific interface based on its membership within a specific VLAN is working on the switch.

Action Display the detailed statistics for MAC addresses that have been learned:

```
user@switch> show ethernet-switching statistics mac-learning interface ge-0/0/28 detail
```

```
Interface: ge-0/0/28.0
Learning message from local packets: 0
Learning message from transit packets: 5
Learning message with error: 0
  Invalid VLAN: 0      Invalid MAC: 0
  Security violation: 0    Interface down: 0
  Incorrect membership: 0  Interface limit: 0
  MAC move limit: 0      VLAN limit: 0
                          VLAN membership limit: 20
  Invalid VLAN index: 0    Interface not learning: 0
  No nexthop: 0          MAC learning disabled: 0
  Others: 0
```

Meaning The **VLAN membership limit** shows the number of packets that were dropped because of the VLAN membership MAC limit for interface ge-0/0/28.0 was exceeded. In this case, 20 packets were dropped.

Verifying That Allowed MAC Addresses Are Working Correctly

Purpose Verify that allowed MAC addresses are working on the switch.

Action Display the MAC address cache information after allowed MAC addresses have been configured on an interface. The following sample shows the MAC address cache after 5 allowed MAC addresses were on interface ge-0/0/2. In this instance, the interface was also set to a dynamic MAC limit of 4 with the default action **drop**.

```
user@switch> show ethernet-switching table
```

```
Ethernet-switching table: 5 entries, 4 learned
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

Meaning Because the MAC limit value for this interface was set to 4, only four of the five configured allowed addresses were learned and thus added to the MAC address cache. Because the fifth address was not learned, an asterisk (*) rather than an address appears in the **MAC address** column in the last line of the sample output.

Verifying Results of Various Action Settings When the MAC Limit Is Exceeded

Purpose Verify the results provided by the various action settings for MAC limits—**drop**, **log**, **shutdown** and **none**—when the limits are exceeded.

Action Display the results of the various action settings.



NOTE: You can view log messages by using the `show log messages` command. You can also have the log messages displayed by configuring the `monitor start messages` with the `monitor start messages` command.

- **drop** action—For MAC limiting configured with a **drop** action and with the MAC limit set to 5:

```
user@switch> show ethernet-switching table
```

Ethernet-switching table: 6 entries, 5 learned				
VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	–	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:88	Learn	0	ge-0/0/2.0

- **log** action—For MAC limiting configured with a **log** action and with MAC limit set to 5:

```
user@switch> show ethernet-switching table
```

Ethernet-switching table: 74 entries, 73 learned				
VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	–	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:82	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:84	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:87	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:88	Learn	0	ge-0/0/2.0
. . .				

- **shutdown** action—For MAC limiting configured with a **shutdown** action and with MAC limit set to 3:

```
user@switch> show ethernet-switching table
```

Ethernet-switching table: 4 entries, 3 learned				
VLAN	MAC address	Type	Age	Interfaces

employee-vlan	*	Flood	-	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:82	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:84	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:87	Learn	0	ge-0/0/2.0

- **none** action—If you set a MAC limit to apply to all interfaces on the switch, you can override that setting for a particular interface by specifying this action for that interface. See [“Override a MAC Limit Applied to All Interfaces” on page 364](#).

Meaning For the **drop** action results—The sixth MAC address exceeded the MAC limit. The request packet for that address was dropped. Only five MAC addresses have been learned on ge-0/0/2.

For the **log** action results—The sixth MAC address exceeded the MAC limit. No MAC addresses were blocked.

For the **shutdown** action results—The fourth MAC address exceeded the MAC limit. Only three MAC addresses have been learned on ge-0/0/2. The interface ge-0/0/1 is shut down.

For more information about interfaces that have been shut down, use the **show ethernet-switching interfaces** command.

```
user@switch> show ethernet-switching interfaces
```

Interface	State	VLAN members	Tag	Tagging	Blocking
bme0.32770	down	mgmt		untagged	unblocked
ge-1/0/0.0	down	v1		untagged	MAC limit exceeded
ge-1/0/1.0	up	v1		untagged	unblocked
ge-1/0/2.0	up	v1		untagged	unblocked
me0.0	up	mgmt		untagged	unblocked



NOTE: You can configure the switch to recover automatically from this type of error condition by specifying the **port-error-disable** statement with a **disable timeout** value. The switch automatically restores the disabled interface to service when the disable timeout expires. The **port-error-disable** configuration does not apply to already existing error conditions. It impacts only error conditions that are detected after **port-error-disable** has been enabled and committed. To clear an already existing error condition and restore the interface to service, use the **clear ethernet-switching port-error** command.

Verifying That Interfaces Are Shut Down

Purpose Verify that an interface is shut down when the MAC limit is exceeded.

Action For more information about interfaces that have been shut down because the MAC limit was exceeded, use the **show ethernet-switching interfaces** command.

```
user@switch> show ethernet-switching interfaces
```

Interface	State	VLAN members	Tag	Tagging	Blocking
bme0.32770	down	mgmt	untagged	unblocked	
xe-0/0/0.0	down	v1	untagged	MAC limit exceeded	
xe-0/0/1.0	up	v1	untagged	unblocked	
xe-0/0/2.0	up	v1	untagged	unblocked	
me0.0	up	mgmt	untagged	unblocked	



NOTE: You can configure interfaces to recover automatically when the MAC limit has been exceeded by specifying the **port-error-disable** statement with a **disable timeout** value. The switch automatically restores the disabled interface to service when the disable timeout expires. The **port-error-disable** configuration does not apply to preexisting error conditions—it affects only error conditions that are detected after the **port-error-disable** statement has been enabled and the configuration has been committed. To clear a preexisting error condition and restore the interface to service, use the **clear ethernet-switching port-error** command.

Customizing the Ethernet Switching Table Display to View Information for a Specific Interface

Purpose You can use the **show ethernet-switching table** command to view information about the MAC addresses learned on a specific interface.

Action For example, to display the MAC addresses learned on ge-0/0/2 interface, type:

```
user@switch> show ethernet-switching table interface ge-0/0/2.0
```

```
Ethernet-switching table: 1 unicast entries
```

VLAN	MAC address	Type	Age	Interfaces
v1	*	Flood	-	All-members

v1	00:00:06:00:00:00 Learn	0 ge-2/0/0.0
----	-------------------------	--------------

Meaning The MAC limit value for ge-0/0/2 was set to 1, and the output shows that only one MAC address was learned and thus added to the MAC address cache. An asterisk (*) rather than an address appears in the **MAC address** column in the first line of the sample output.

- Related Documentation**
- [Configuring MAC Limiting \(non-ELS\) on page 341](#)
 - [Configuring Autorecovery for Port Security Events on page 635](#)
 - [Example: Protecting Against DHCP Snooping Database Attacks on page 415](#)
 - [Example: Protecting against Ethernet Switching Table Overflow Attacks on page 354](#)
 - [Example: Protecting against DHCP Starvation Attacks on page 347](#)
 - [Monitoring Port Security](#)

Override a MAC Limit Applied to All Interfaces

If you set a MAC limit in your port security settings to apply to all interfaces on the EX Series switch, you can override that setting for a particular interface by specifying action the **none**.

To use the **none** action to override a MAC limit setting:

1. Set the MAC limit for all interfaces to have a limit of, for example, **5** using the action **drop**:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all mac-limit 5 action drop
```

2. Then change the action for one interface (here, **ge-0/0/2**) with this command. You don't need to specify a limit value.

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/2 mac-limit action none
```



NOTE: In MX and SRX series devices, the 1 and 10-Gigabit SFP or SFP+ optical interfaces are always named as xe even if a 1-Gigabit SFP is inserted. However, in EX and QFX series devices, the interface name is shown as ge or xe based on the speed of the optical device inserted.

- Related Documentation**
- [Configuring MAC Limiting \(non-ELS\) on page 341](#)
 - [Example: Configuring Port Security \(non-ELS\) on page 15](#)

- [Verifying That MAC Limiting Is Working Correctly on page 357](#)
- [Example: Protecting against Ethernet Switching Table Overflow Attacks on page 354](#)
- [Example: Protecting against DHCP Starvation Attacks on page 347](#)

Configuring MAC Move Limiting (ELS)



NOTE: This topic uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

When MAC move limiting is configured, the switch tracks MAC address movements on access and trunk interfaces. A MAC address move occurs when the switch receives a packet with a source MAC address that has already been learned by the switch, but on a different interface. If a MAC address changes more than the configured number of times within one second, the changes to MAC addresses are dropped, logged or ignored, or the interface is shut down, as specified in the configuration.

MAC move limiting is not configured by default.

You can choose to have one of the following actions performed when the MAC move limit is exceeded:

- **drop**—(EX2300, EX3400 and EX4300) Drop the packet, but do not generate an alarm.
- **drop-and-log**—(EX2300, EX3400 and EX4300 only) Drop the packet and generate an alarm, an SNMP trap, or system log entry.
- **log**—(EX4300 and EX9200) Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- **none**—(EX4300 and EX9200) Forward packets with new source MAC addresses, and learn the new source MAC address.
- **shutdown**—Disable the interface in the VLAN and generate an alarm, an SNMP trap, or a system log entry. If you configure an interface with the [recovery-timeout](#) statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you do not configure the switch for autorecovery from the disabled condition, you can bring up the disabled interfaces by running the [clear ethernet-switching recovery-timeout](#) command.
- **vlan-member-shutdown**—(EX9200 only) Block an interface on the basis of its membership in a specific VLAN and generate an alarm, an SNMP trap, or a system log entry. If you configure an interface with the [recovery-timeout](#) statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you do not configure [recovery-timeout](#), then the interface remains blocked for 180 seconds, after which it is automatically restored. You can recover all of the blocked interfaces by running the [clear ethernet-switching recovery-timeout](#) command, or recover a specific interface by using the [set ethernet-switching recovery-timeout interface interface-name vlan vlan-name](#) command.

To configure a MAC move limit for MAC addresses within a specific VLAN:

- To limit the number of MAC address movements that can be made by an individual MAC address within the specified VLAN:

```
[edit edit vlans vlan-name switch-options]
user@switch# set mac-move-limit limit
```

- To limit the number of MAC address movements that can be made by an individual MAC address and to specify the action to be taken when the limit is reached:

```
[edit edit vlans vlan-name switch-options]
user@switch# set mac-move-limit limit packet-action action
```

The switch performs the specified action if it tracks that an individual MAC address within the specified VLAN has moved more than the specified number of times within one second.

- Starting in Junos OS Release 15.1 for EX9200 Switches with configured actions for MAC Move Limiting, you can determine the priority for an interface involved in the MAC move to be selected for the action. To determine the priority for an interface involved in the MAC move:

```
[edit edit vlans vlan-name switch-options]
user@switch# set mac-move-limit interface interface-name action-priority value
```

The interface with the lowest value configured for **action-priority** has the highest priority.



NOTE: You can use the action priority to decrease the likelihood of blocking a trusted interface. The trusted interface should have the lowest priority if the configured action is **shutdown** or **vlan-member-shutdown**. To assign a low priority, configure a high value for **action-priority**.

Release History Table

Release	Description
15.1	Starting in Junos OS Release 15.1 for EX9200 Switches with configured actions for MAC Move Limiting, you can determine the priority for an interface involved in the MAC move to be selected for the action.

Related Documentation

- [Understanding MAC Limiting and MAC Move Limiting on page 330](#)
- [Configuring MAC Limiting \(ELS\)](#)
- [Configuring Persistent MAC Learning \(ELS\) on page 337](#)

Verifying That MAC Move Limiting Is Working Correctly

Purpose Verify that MAC move limiting is working on the switch.

Action Display the MAC addresses in the Ethernet switching table when MAC move limiting has been configured for a VLAN. The following sample shows the results after two of the hosts on **ge-0/0/2** sent packets after the MAC addresses for those hosts had moved to other interfaces more than five times in 1 second. The VLAN, **employee-vlan**, was set to a MAC move limit of 5 with the action **drop**:

user@switch> [show ethernet-switching table](#)

```
Ethernet-switching table: 7 entries, 4 learned
VLAN          MAC address      Type      Age      Interfaces
employee-vlan 00:05:85:3A:82:77 Learn      0      ge-0/0/1.0
employee-vlan 00:05:85:3A:82:79 Learn      0      ge-0/0/1.0
employee-vlan 00:05:85:3A:82:80 Learn      0      ge-0/0/2.0
employee-vlan 00:05:85:3A:82:81 Learn      0      ge-0/0/2.0
employee-vlan *              Flood     -      ge-0/0/2.0
employee-vlan *              Flood     -      ge-0/0/2.0
```

Meaning The last two lines of the sample output show that MAC addresses for two hosts on **ge-0/0/2** were not learned, because the hosts had been moved back and forth from the original interfaces more than five times in 1 second.

- Related Documentation**
- [Configuring MAC Move Limiting \(non-ELS\)](#)
 - [Configuring MAC Move Limiting \(J-Web Procedure\)](#)
 - [Configuring Autorecovery for Port Security Events on page 635](#)
 - [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [Monitoring Port Security](#)

Verifying That the Port Error Disable Setting Is Working Correctly

Purpose Verify that the port error disable setting is working as expected for MAC limited, MAC move limited, and rate-limited interfaces on an EX Series switch, or that MAC limited and storm control interfaces are working as expected for QFX Series switches or NFX Series devices.

Action Display information about interfaces:

```
user@switch> show ethernet-switching interfaces
```

Interface	State	VLAN members	Blocking
ge-0/0/0.0	up	T1122	unblocked
ge-0/0/1.0	down	default	MAC limit exceeded
ge-0/0/2.0	down	default	MAC move limit exceeded
ge-0/0/3.0	down	default	Storm control in effect
ge-0/0/4.0	down	default	unblocked

Meaning For interfaces disabled by port security features, the sample output from the **show ethernet-switching interfaces** command shows the reason that the down interface is disabled:

- **MAC limit exceeded**—The interface is temporarily disabled because of a MAC limit error. The disabled interface is automatically restored to service when the **disable-timeout** expires.
- **MAC move limit exceeded**—The interface is temporarily disabled because of a MAC move limit error. The disabled interface is automatically restored to service when the **disable-timeout** expires.
- **Storm control in effect** —The interface is temporarily disabled because of a storm control error. The disabled interface is automatically restored to service when the **disable-timeout** expires.

Related Documentation

- [Configuring Autorecovery for Port Security Events on page 635](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security](#)
- [mac-limit on page 851](#)
- [mac-move-limit on page 854](#)
- [disable-timeout on page 742](#)

PART 6

DHCP Protection

- [DHCPv4 and DHCPv6 on page 371](#)
- [DHCP Snooping on page 385](#)
- [DHCP Option 82 on page 429](#)

CHAPTER 14

DHCPv4 and DHCPv6

- [Understanding and Using Trusted DHCP Servers on page 371](#)
- [Example: Protecting against Rogue DHCP Server Attacks on page 374](#)
- [DHCPv6 Rapid Commit on page 378](#)
- [Using Lightweight DHCPv6 Relay Agent \(LDRA\) on page 379](#)
- [Configuring Persistent Bindings in the DHCP or DHCPv6 \(ELS\) on page 381](#)
- [Configuring Persistent Bindings in the DHCP or DHCPv6 \(non-ELS\) on page 383](#)

Understanding and Using Trusted DHCP Servers

- [Understanding Trusted and Untrusted Ports and DHCP Servers on page 371](#)
- [Enabling a Trusted DHCP Server \(ELS\) on page 372](#)
- [Enabling a Trusted DHCP Server \(non-ELS\) on page 373](#)
- [Enabling a Trusted DHCP Server \(MX Series Routers\) on page 373](#)
- [Verifying That a Trusted DHCP Server Is Working Correctly on page 374](#)

Understanding Trusted and Untrusted Ports and DHCP Servers

DHCP servers provide IP addresses and other configuration information to the network's DHCP clients. Using trusted ports for the DHCP server protects against rogue DHCP servers sending leases.

Untrusted ports drop traffic from DHCP servers to prevent unauthorized servers from providing any configuration information to clients.

By default, all trunk ports are trusted for DHCP and all access ports are untrusted.

You can configure an override of the default behavior to set a trunk port as untrusted, which blocks all ingress DHCP server messages from that interface. This is useful for preventing a rogue DHCP server attack, in which an attacker has introduced an unauthorized server into the network. The information provided to DHCP clients by this server has the potential to disrupt their network access. The unauthorized server might also assign itself as the default gateway device for the network. An attacker can then sniff the network traffic and perpetrate a man-in-the-middle attack—that is, it misdirects traffic intended for a legitimate network device to a device of its choice.

You can also configure an access port as trusted. If you attach a DHCP server to an access port, you must configure the port as trusted. Before you do so, ensure that the server is physically secure—that is, that access to the server is monitored and controlled.

Enabling a Trusted DHCP Server (ELS)



NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style.

You can configure any interface on a switch that connects to a DHCP server as a trusted interface (port). Configuring a DHCP server on a trusted interface protects against rogue DHCP servers sending leases.

By default, all access interfaces are untrusted, and all trunk interfaces are trusted. However, you can override the default setting for access interfaces by configuring a group of access interfaces within a VLAN, specifying an interface to belong to that group, and then configuring the group as trusted.

Before you can configure a trusted DHCP server, you must configure a VLAN. See *Configuring VLANs for EX Series Switches with ELS Support (CLI Procedure)*.

To configure an untrusted access interface as a trusted interface for a DHCP server by using the CLI :

1. Configure a group within a VLAN with a specific access interface:

```
[edit vlans vlan-name forwarding-options dhcp-security ]  
user@switch# set group group-name interface interface-name
```

2. Configure that group as **trusted** to make the specified interface contained within the group a trusted interface:

```
[edit vlans vlan-name forwarding-options dhcp-security group group-name]  
user@switch# set overrides trusted
```


Enabling a Trusted DHCP Server (non-ELS)

You can protect against rogue DHCP servers sending rogue leases on your network by using trusted DHCP servers and ports. By default, for DHCP, all trunk ports are trusted, and all access ports are untrusted. And you can only set up DHCP server on an interface; that is, using a VLAN is not supported.

Trusted ports allow DHCP servers to provide IP addresses and other information to requesting devices. Untrusted ports drop traffic from DHCP servers to prevent unauthorized servers from providing any configuration information to clients.

To configure a port to host a DHCP server, enter the following command from the Junos CLI:

```
[edit ethernet-switching-options secure-access port]
user@switch# set interface ge-0/0/8 dhcp-trusted
```

where, the interface, **ge-0/0/8** is any trusted and physically secure interface that is valid for your network.

- See Also**
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [Monitoring Port Security](#)

Enabling a Trusted DHCP Server (MX Series Routers)

You can configure any interface on a switching device that connects to a DHCP server as a trusted interface (port). Configuring a DHCP server on a trusted interface protects against rogue DHCP servers sending leases.

By default, all access interfaces are untrusted, and all trunk interfaces are trusted. However, you can override the default setting for access interfaces by configuring a group of access interfaces within a bridge domain, specifying an interface to belong to that group, and then configuring the group as trusted.

Before you can configure a trusted DHCP server, you must configure a bridge domain.

To configure an untrusted access interface as a trusted interface for a DHCP server by using the CLI :

1. Configure a group within a bridge domain with a specific access interface:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security]
user@device# set group group-name interface interface-name
```

2. Configure that group as **trusted** to make the specified interface contained within the group a trusted interface:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security group
group-name]
user@device# set overrides trusted
```

Verifying That a Trusted DHCP Server Is Working Correctly

Purpose Verify that a DHCP trusted server is working on the switch. See what happens when the DHCP server is trusted and then untrusted.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

user@switch> **show dhcp snooping binding**

DHCP Snooping Information:

MAC Address	IP Address	Lease	Type	VLAN	Interface
00:05:85:3A:82:77	192.0.2.17	600	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:79	192.0.2.18	653	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:80	192.0.2.19	720	dynamic	employee-vlan	ge-0/0/2.0
00:05:85:3A:82:81	192.0.2.20	932	dynamic	employee-vlan	ge-0/0/2.0
00:05:85:3A:82:83	192.0.2.21	1230	dynamic	employee-vlan	ge-0/0/2.0
00:05:85:27:32:88	192.0.2.22	3200	dynamic	employee-vlan	ge-0/0/2.0

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

If the DHCP server had been configured as untrusted, no entries would be added to the DHCP snooping database and nothing would be shown in the output of the **show dhcp snooping binding** command.

See Also

- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Example: Protecting against Rogue DHCP Server Attacks on page 351](#)
- *Monitoring Port Security*
- *Troubleshooting Port Security*

Example: Protecting against Rogue DHCP Server Attacks

In a rogue DHCP server attack, an attacker has introduced a rogue server into the network, allowing it to give IP address leases to the network's DHCP clients and to assign itself as the gateway device.

This example describes how to configure a DHCP server interface as untrusted to protect the switch from a rogue DHCP server:

- [Requirements on page 375](#)
- [Overview and Topology on page 375](#)
- [Configuration on page 376](#)
- [Verification on page 377](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch or one QFX3500 switch
- Junos OS Release 9.0 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure an untrusted DHCP server interface to mitigate rogue DHCP server attacks, be sure you have:

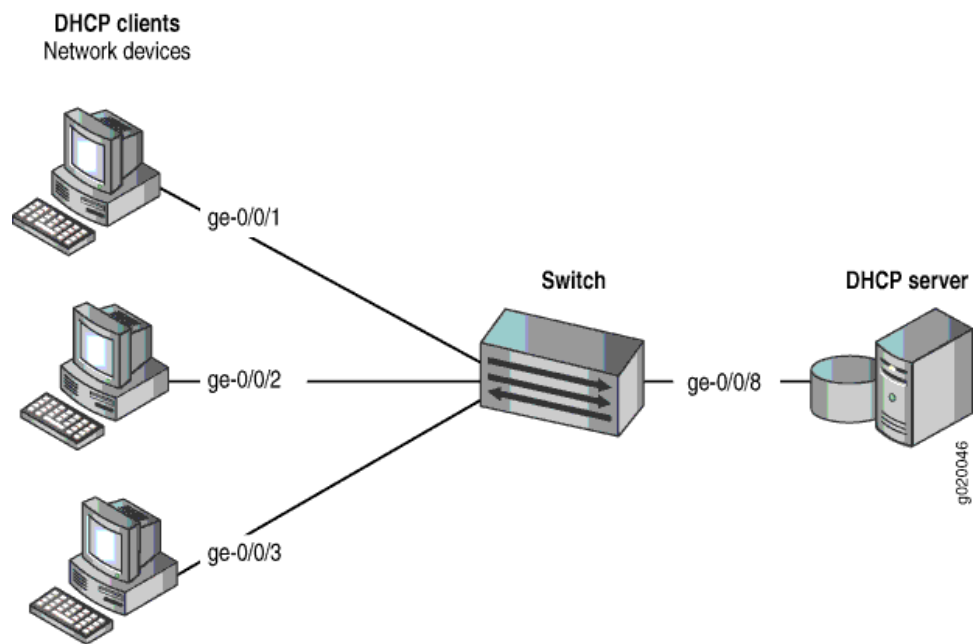
- Connected the DHCP server to the switch.
- Enabled DHCP snooping on the VLAN.
- Configured a VLAN on the switch. See the task for your platform:
 - *Example: Setting Up Bridging with Multiple VLANs.*

Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch from rogue DHCP server attacks.

This example shows how to explicitly configure an untrusted interface on an EX3200-24P switch and a QFX3500 switch. [Figure 14 on page 352](#) illustrates the topology for this example.

Figure 16: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 18 on page 352](#).

Table 20: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	employee-vlan , tag 20
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is the subnet's broadcast address
Interfaces in employee-vlan	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface for DHCP server	ge-0/0/8

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- DHCP snooping is enabled on the VLAN **employee-vlan**.
- The interface (port) where the rogue DHCP server has connected to the switch is currently trusted.

Configuration

To configure the DHCP server interface as untrusted because the interface is being used by a rogue DHCP server:

CLI Quick Configuration To quickly set the rogue DHCP server interface as untrusted, copy the following command and paste it into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/8 no-dhcp-trusted
```

Step-by-Step Procedure To set the DHCP server interface as untrusted:

- Specify the interface (port) from which DHCP responses are not allowed:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/8 no-dhcp-trusted
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/8.0 {
  no-dhcp-trusted;
}
```

Verification

Confirm that the configuration is working properly.

Verifying That the DHCP Server Interface Is Untrusted

Purpose Verify that the DHCP server is untrusted.

- Action**
1. Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.
 2. Display the DHCP snooping information when the port on which the DHCP server connects to the switch is not trusted.

Meaning There is no output from the command because no entries are added to the DHCP snooping database.

- Related Documentation**
- [Understanding and Using Trusted DHCP Servers on page 371](#)
 - [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [show dhcp snooping binding on page 1178](#)

DHCPv6 Rapid Commit

- [Configuring DHCPv6 Rapid Commit \(MX, EX\) on page 378](#)
- [Configuring the DHCPv6 Client Rapid Commit Option on page 378](#)

Configuring DHCPv6 Rapid Commit (MX, EX)

You can configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option (DHCPv6 option 14). When rapid commit is enabled, the server recognizes the Rapid Commit option in Solicit messages sent from the DHCPv6 client. (DHCPv6 clients are configured separately to include the DHCPv6 Rapid Commit option in the Solicit messages.) The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-message exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

You can configure the DHCPv6 local server to support the Rapid Commit option globally, for a specific group, or for a specific interface. By default, rapid commit support is disabled on the DHCPv6 local server.

To configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option:

1. Specify that you want to configure the **overrides** options:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit overrides
```

2. Enable rapid commit support:

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set rapid-commit
```

See Also • [Overriding the Default DHCP Local Server Configuration Settings Overview](#)

Configuring the DHCPv6 Client Rapid Commit Option

The DHCPv6 client can obtain configuration parameters from a DHCPv6 server through a rapid two-message exchange (solicit and reply). When the rapid commit option is enabled by both the DHCPv6 client and the DHCPv6 server, the two-message exchange is used, rather than the default four-method exchange (solicit, advertise, request, and reply). The two-message exchange provides faster client configuration and is beneficial in environments in which networks are under a heavy load.

To configure the DHCPv6 client to support the DHCPv6 rapid commit option on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the two-message exchange option for address assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set rapid-commit
```

Using Lightweight DHCPv6 Relay Agent (LDRA)

In Layer 2 networks that have many nodes on a single link, a DHCP server would normally be unaware of how a DHCP client is attached to the network. In a DHCPv6 deployment, you can use a Lightweight DHCPv6 Relay Agent (LDRA) to add relay agent information to a DHCPv6 message to identify the client-facing interface of the access node that received the message. The server can use this information to assign IP addresses, prefixes, and other configuration parameters for the client.

DHCPv6 relay agents are typically used to forward DHCPv6 messages between clients and servers or other relay agents when they are not on the same IPv6 link node. The relay agent can add information to the messages before relaying them. When the client and server reside on the same IPv6 link, LDRA enables a switching device to perform the function of intercepting DHCPv6 messages and inserting relay agent information that can be used for client identification. The LDRA acts as a relay agent, but without performing the routing function necessary to forward messages to a server or relay agent that resides on a different IPv6 link.

When the LDRA receives a DHCPv6 Solicit message from a client, it encapsulates that message within a DHCPv6 Relay-Forward message, which it then forwards to the server or another relay agent. Before it forwards the Relay-Forward message, the LDRA can also insert relay information by using one or more of the following options:

- **option-16** (Vendor ID)—Option 16 provides the server with information about the vendor that manufactured the hardware on which the DHCPv6 client is running. Option 16 is the DHCPv6 equivalent of the **vendor-id** suboption of DHCP option 82.
- **option-18** (Interface ID)—A unique identifier for the interface on which the client DHCPv6 packet is received. Suboptions can be configured to include a prefix with the interface ID or to change the type of information used to identify the interface. Option 18 is the DHCPv6 equivalent of the **circuit-id** suboption of DHCP option 82.
- **option-37** (Remote ID)—A unique identifier for the remote host. Suboptions can be configured to include a prefix with the remote ID or to change the interface portion of the ID. Option 37 is the DHCPv6 equivalent of the **remote-id** suboption of DHCP option 82.

You must configure LDRA if you configure DHCPv6 options at the **[edit vlan *vlan-name* forwarding-options dhcp-security dhcpv6-options]** hierarchy level. Option 16, option 37, and option 79 are included in the Relay-Forward message only if they are explicitly configured. Option 18 is mandatory in Relay-Forward messages and is included even if

it is not explicitly configured. However, suboptions of option 18 are included only if they are configured using the **option-18** statement at the **[edit vlan *vlan-name* forwarding-options dhcp-security dhcpv6-options]** hierarchy level.

To configure LDRA to enable DHCPv6 options:

1. Configure the switch as an LDRA.

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set light-weight-dhcpv6-relay
```

2. Configure the switch to insert DHCPv6 options in the Relay-Forward message to provide additional information about the client to the server or to another relay agent.

- To insert option 16:

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set dhcpv6-options option-16
```

- To insert option 18:

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set dhcpv6-options option-18
```

- To insert option 37:

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set dhcpv6-options option-37
```

3. (Optional) Configure a prefix to include additional information with DHCPv6 option 18 or DHCPv6 option 37. For example, to configure a prefix for option 37 to include the switch's hostname:

```
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options]
user@switch# set option-37 prefix host-name
```

4. (Optional) Change the type of information used to identify the interface. For example, to specify that option 18 contain the interface description for the logical unit rather than the interface name (the default):

```
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options]
user@switch# set option-18 use-interface-description logical
```



NOTE: To use the interface description rather than the interface name for identifying the interface, the interface description must be specified under interface unit (**set interfaces *ge-0/0/0* unit 0 description *description***). If you do not do this, then the interface name is used by default.

Related Documentation

- [Understanding DHCP Option 82 on page 429](#)

Configuring Persistent Bindings in the DHCP or DHCPv6 (ELS)



NOTE: This task uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see [“Configuring Persistent Bindings in the DHCP or DHCPv6 \(non-ELS\)”](#) on page 383. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

By default, IP-MAC address bindings in the DHCP snooping database do not persist through device reboots. You can improve network performance by configuring the IP-MAC address bindings in the DHCP snooping database to persist through reboots so that the table does not need to be rebuilt after rebooting. Do this by configuring a storage location for the DHCP snooping database file, where you must specify how frequently the device writes the database entries into the DHCP snooping database file.



NOTE: You can also configure persistent bindings for IPv6 addresses and MAC addresses on devices that support DHCPv6 snooping.

DHCPv6 is not supported on the MX Series routers.

The DHCP snooping database of IP-MAC bindings is created when you enable any of the port security features for a specific VLAN or bridge domain in either of the following hierarchy levels:

- [edit vlans *vlan-name* forwarding-options dhcp-security]
- [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]

On devices that support DHCPv6, enabling any port security features will automatically enable DHCPv6 snooping. DHCP snooping and DHCPv6 snooping are not enabled by default.

To configure a *local* storage location for the DHCP snooping database file:

- For DHCP snooping:

```
[edit system processes]
user@device# set dhcp-service dhcp-snooping-file local-pathname write-interval seconds
```

For example:

```
[edit system processes]
user@device# set dhcp-service dhcp-snooping-file /var/tmp/test.log write-interval 60
```

- For DHCPv6 snooping:

```
[edit system processes]
user@device# set dhcp-service dhcpv6-snooping-file local-pathname write-interval seconds
```

For example:

```
[edit system processes]
user@device# set dhcp-service dhcpv6-snooping-file /var/tmp/test.log write-interval 60
```

To configure a *remote* storage location for IP-MAC bindings, use **tftp://*ip-address*** or **ftp://*hostname/path*** as the remote URL, or the local pathname for the storage location of the DHCP or DHCPv6 snooping database file:

- For DHCP snooping:

```
[edit system processes]
user@device# set dhcp-service dhcp-snooping-file remote_url write-interval seconds
```

For example:

```
[edit system processes]
user@device# set dhcp-service dhcp-snooping-file tftp://@14.1.2.1 write-interval 60
```

- For DHCPv6 snooping:

```
[edit system processes]
user@device# set dhcp-service dhcpv6-snooping-file remote_url write-interval seconds
```

For example:

```
[edit system processes]
user@device# set dhcp-service dhcpv6-snooping-file tftp://@14.1.2.1 write-interval 60
```

Related Documentation

- [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

Configuring Persistent Bindings in the DHCP or DHCPv6 (non-ELS)



NOTE: This task uses Junos OS without support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see [“Configuring Persistent Bindings in the DHCP or DHCPv6 \(ELS\)”](#) on [page 381](#) instead. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

By default, IP-MAC bindings in the DHCP snooping database do not persist through switch reboots. You can configure the IP-MAC bindings in the DHCP snooping database to persist through switch reboots by configuring a storage location for the DHCP snooping database file. When specifying the location for the DHCP snooping database, you must also specify how frequently the switch writes the database entries into the DHCP snooping database file.

The DHCP snooping database of IP-MAC bindings is created when you enable DHCP snooping. DHCP snooping is not enabled by default. You can configure DHCP snooping on a specific VLAN or on all VLANs. See [“Enabling DHCP Snooping \(non-ELS\)”](#) on [page 400](#).

To configure a local storage location for the DHCP snooping database file:

- For DHCPv4 snooping:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcp-snooping-file location local-pathname write-interval
seconds
```

For example:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcp-snooping-file location /var/tmp/test.log
write-interval 60
```

- For DHCPv6 snooping:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcpv6-snooping-file location local-pathname
write-interval seconds
```

For example:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcpv6-snooping-file location /var/tmp/test.log
write-interval 60
```

To configure a remote storage location for IP-MAC bindings, use `tftp://ip-address` or `ftp://hostname/path` as the remote URL or the local pathname for the storage location of the DHCP or DHCPv6 snooping database file:

- For DHCPv4 snooping:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcp-snooping-file location remote_url write-interval
seconds
```

For example:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcp-snooping-file location ftp://test:Test123@14.1.2.1
write-interval 60
```

- For DHCPv6 snooping:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcpv6-snooping-file location remote_url write-interval
seconds
```

For example:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port dhcpv6-snooping-file location ftp://test:Test123@14.1.2.1
write-interval 60
```



NOTE: If you save the DHCP or DHCPv6 snooping file to a remote server using TFTP, then the CLI returns a message that the save process is initiated. The CLI remains accessible during the save process; however, if you attempt to save a file while the previous save is still pending, the CLI returns an error message.



NOTE: Specify any requisite user credentials for the FTP server before you specify the IP address or hostname. In this example, **test** is the username and **Test123** is the password for FTP server 14.1.2.1.

When you are storing the DHCP snooping database at a remote location, you might also want to specify a timeout value for remote read and write operations. See [timeout](#). This configuration is optional.

Release History Table

Release	Description
14.1X53-D40	If you save the DHCP or DHCPv6 snooping file to a remote server using TFTP, then the CLI returns a message that the save process is initiated.

**Related
Documentation**

- [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

DHCP Snooping

- [Understanding DHCP Snooping \(ELS\) on page 385](#)
- [Understanding DHCP Snooping \(non-ELS\) on page 393](#)
- [Enabling DHCP Snooping \(non-ELS\) on page 400](#)
- [Configuring Static DHCP IP Addresses on page 403](#)
- [Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks on page 406](#)
- [Example: Protecting Against DHCP Snooping Database Attacks on page 415](#)
- [Example: Protecting Against ARP Spoofing Attacks on page 418](#)
- [Example: Prioritizing Snooped and Inspected Packet on page 423](#)

Understanding DHCP Snooping (ELS)



NOTE: This topic includes information about enabling Dynamic Host Configuration Protocol (DHCP) snooping when using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs Junos OS software that does not support ELS, see [“Understanding DHCP Snooping \(non-ELS\)” on page 393](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

DHCP snooping enables the switching device, which can be either a switch or a router, to monitor DHCP messages received from untrusted devices connected to the switching device. When DHCP snooping is enabled on a VLAN, the system examines DHCP messages sent from untrusted hosts associated with the VLAN and extracts their IP addresses and lease information. This information is used to build and maintain the DHCP snooping database. Only hosts that can be verified using this database are allowed access to the network.

- [DHCP Snooping Basics on page 386](#)
- [Enabling DHCP Snooping on page 387](#)
- [DHCP Snooping Process on page 387](#)
- [DHCPv6 Snooping on page 388](#)
- [Rapid Commit for DHCPv6 on page 389](#)

- [DHCP Server Access on page 389](#)
- [Static IP Address Additions to the DHCP Snooping Database on page 392](#)

DHCP Snooping Basics

DHCP allocates IP addresses dynamically, *leasing* addresses to devices so that the addresses can be reused when they are no longer needed by the devices to which they were assigned. Hosts and end devices that require IP addresses obtained through DHCP must communicate with a DHCP server across the LAN.

DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server (the server is connected to a trusted network port).

By default, all trunk ports on the switch are trusted and all access ports are untrusted for DHCP snooping.



NOTE: You can configure an access port as trusted, or a trunk port as untrusted, using the **overrides** configuration statement with either the **trusted** or **untrusted** option.

When DHCP snooping is enabled, the lease information from the server is used to create the DHCP snooping table, also known as the DHCP binding table. The table shows current IP-MAC address bindings, as well as lease time, type of binding, names of associated VLANs and interfaces.

Entries in the DHCP snooping table are updated in the following events:

- When a network device releases an IP address (sends a DHCPRELEASE message). In this event, the associated mapping entry is deleted from the database.
- When you move a network device from one VLAN to another. In this event, typically the device needs to acquire a new IP address. Therefore, its entry in the database, including the VLAN name, is updated.
- When the lease time (timeout value) assigned by the DHCP server expires. In this event, the associated entry is deleted from the database.
- When the network device renews its lease by sending a unicast DHCPREQUEST message and receiving a positive response from the DHCP server. In this event, the lease time is updated in the database.
- If the network device cannot reach the DHCP server that originally granted the lease, it sends a broadcast DHCPREQUEST message and rebinds to the DHCP server that responds. In this event, the client receives a new IP address and the binding is updated in the DHCP snooping table.
- Starting in Junos OS Release 14.1X53-D35, a network device with a fixed IP allocation from the DHCP server is replaced by a new device with a different MAC address. If a network device with a fixed IP allocation from the DHCP server is replaced by a new device with a different MAC address. In this event, the new IP-MAC address binding is

stored until the server sends a DHCPACK message, and then the entry in the DHCP snooping table is updated with the new address binding.



TIP: By default, the IP-MAC bindings are lost when the switch is rebooted, and the DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the `dhcp-snooping-file` statement to store the database file either locally or remotely.

You can configure the switch to snoop DHCP server responses only from specific VLANs. Doing this prevents spoofing of DHCP server messages.

Enabling DHCP Snooping

DHCP snooping is not enabled in the default switch configuration. DHCP snooping is enabled automatically by Junos OS when you configure any port security features at the `[edit vlans vlan-name forwarding-options dhcp-security]` hierarchy level. Starting in Junos OS Release 17.1R1, you can configure DHCP snooping or DHCPv6 snooping on a VLAN without enabling other port security features by configuring the `dhcp-security` CLI statement at the `[edit vlans vlan-name forwarding-options dhcp-security]`. You enable DHCP snooping per VLAN, not per interface (port). For additional information about enabling DHCP snooping, see “[Configuring Port Security \(ELS\)](#)” on page 9.



NOTE: To disable DHCP snooping, you must delete the `dhcp-security` statement from the configuration. DHCP snooping is not disabled automatically when you disable other port security features.

DHCP Snooping Process

The DHCP snooping process consists of the following steps:



NOTE: When DHCP snooping is enabled for a VLAN, all DHCP packets sent from network devices in that VLAN are subjected to DHCP snooping. The final IP-MAC binding occurs when the DHCP server sends a DHCPACK packet to the DHCP client.

1. The network device sends a DHCPDISCOVER packet to request an IP address.
2. The switch forwards the packet to the DHCP server.
3. The server sends a DHCPOFFER packet to offer an address. If the DHCPOFFER packet is from a trusted interface, the switch forwards the packet to the network device.

4. The network device sends a DHCPREQUEST packet to accept the IP address. The switch adds an IP-MAC placeholder binding to the DHCP snooping table. The entry is considered a placeholder until a DHCPACK packet is received from the server. Until then, the IP address could still be assigned to some other host.
5. The server sends a DHCPACK packet to assign the IP address or a DHCPNAK packet to deny the address request.
6. The switch updates the DHCP database according to the type of packet received:
 - If the switch receives a DHCPACK packet, it updates lease information for the IP-MAC address bindings in its database.
 - If the switch receives a DHCPNACK packet, it deletes the placeholder.



NOTE: The DHCP database is updated only after the DHCPREQUEST packet is sent.

For general information about the messages that the DHCP client and DHCP server exchange during the assignment of an IP address for the client, see the [Junos OS System Basics Configuration Guide](#).

DHCPv6 Snooping

Starting in Junos OS Release 14.1X53-D10, DHCP snooping is supported for IPv6 packets on EX 9200 Switches. DHCP snooping is also supported for IPv6 packets. The process for DHCPv6 snooping is similar to that for DHCP snooping, but uses different names for the messages exchanged between the client and server to assign IPv6 addresses.

[Table 21 on page 388](#) shows DHCPv6 messages and their DHCPv4 equivalents.

Table 21: DHCPv6 Messages and DHCPv4 Equivalent Messages

Sent by	DHCPv6 Messages	DHCPv4 Equivalent Messages
Client	SOLICIT	DHCPDISCOVER
Server	ADVERTISE	DHCPOFFER
Client	REQUEST, RENEW, REBIND	DHCPREQUEST
Server	REPLY	DHCPACK/DHCPNAK
Client	RELEASE	DHCPRELEASE
Client	INFORMATION-REQUEST	DHCPINFORM
Client	DECLINE	DHCPDECLINE
Client	CONFIRM	none

Table 21: DHCPv6 Messages and DHCPv4 Equivalent Messages (continued)

Sent by	DHCPv6 Messages	DHCPv4 Equivalent Messages
Server	RECONFIGURE	DHCPFORCERENEW
Client	RELAY-FORW, RELAY-REPLY	none

Rapid Commit for DHCPv6

The DHCPv6 Rapid Commit option can shorten the exchange of messages between the client and server. When supported by the server and set by the client, this option shortens the exchange from a four-way relay to a two-message handshake. For more information about enabling the Rapid Commit option, see [“Configuring DHCPv6 Rapid Commit \(MX, EX\)” on page 378](#).

When the Rapid Commit option is enabled, the exchange of messages is as follows:

1. The DHCPv6 client sends out a SOLICIT message that contains a request that rapid assignment of address, prefix, and other configuration parameters be preferred.
2. If the DHCPv6 server supports rapid assignment, it responds with a REPLY message, which contains the assigned IPv6 address and prefix and other configuration parameters.

DHCP Server Access

A switch's access to the DHCP server can be configured in three ways:

- [Switch, DHCP Clients, and the DHCP Server Are All on the Same VLAN on page 389](#)
- [Switch Acts as the DHCP Server on page 391](#)
- [Switch Acts as a Relay Agent on page 391](#)

Switch, DHCP Clients, and the DHCP Server Are All on the Same VLAN

When the switch, DHCP clients, and DHCP server are *all members of the same VLAN*, the DHCP server can be connected to the switch in one of two ways:



NOTE: To enable DHCP snooping on the VLAN, configure the `dhcp-security` statement at the `[edit vlans vlan-name forwarding-options]` hierarchy.

- (See [Figure 17 on page 390](#).) The server is directly connected to the same switch as the one connected to the DHCP clients (the hosts, or network devices, that are requesting IP addresses from the server). The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port.
- (See [Figure 18 on page 390](#).) The server is connected to an intermediary switch (Switch 2) that is connected through a trunk port to the switch (Switch 1) that the DHCP clients are connected to. Switch 2 is being used as a transit switch. The VLAN is enabled for

DHCP snooping to protect the untrusted access ports of Switch 1. The trunk port is configured by default as a trusted port. In [Figure 18 on page 390](#), ge-0/0/11 is a trusted trunk port.

Figure 17: DHCP Server Connected Directly to a Switch

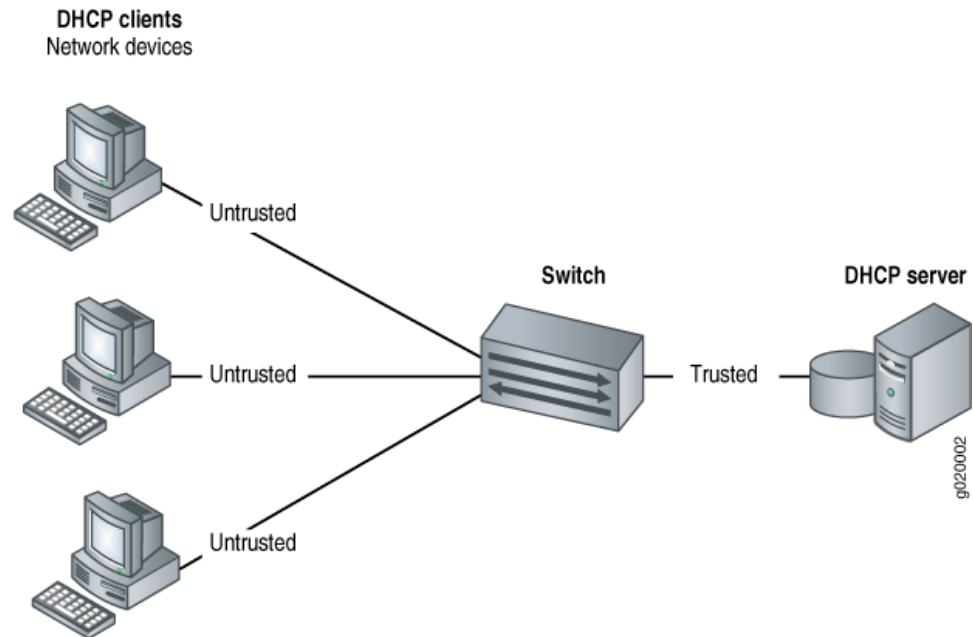
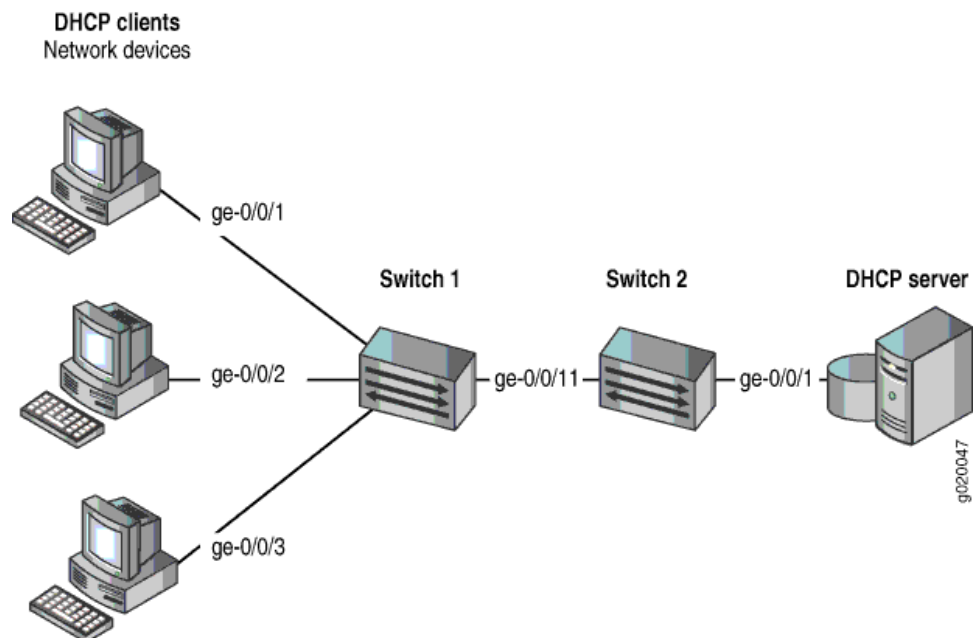


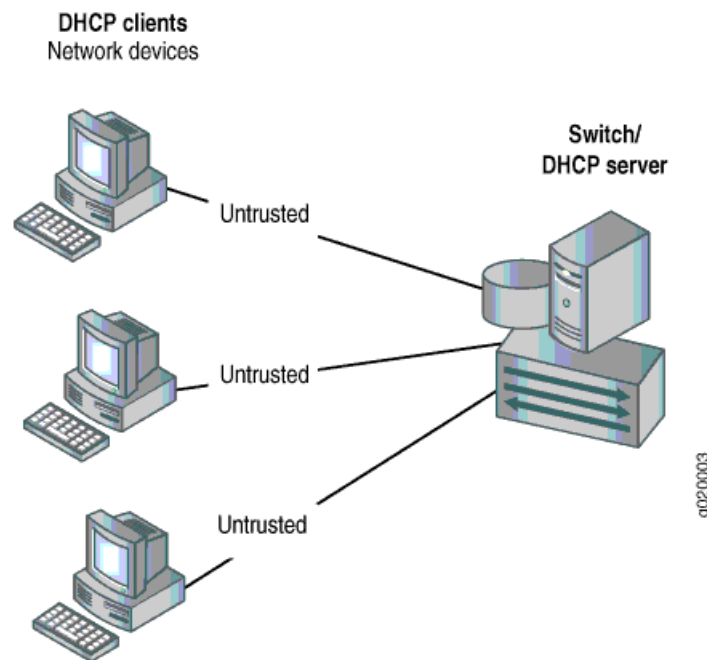
Figure 18: DHCP Server Connected Directly to Switch 2, with Switch 2 Connected to Switch 1 Through a Trusted Trunk Port



Switch Acts as the DHCP Server

You can configure DHCP local server options on the switch, which enables the switch to function as an extended DHCP local server. In [Figure 19 on page 391](#), the DHCP clients are connected to the extended DHCP local server through untrusted access ports.

Figure 19: Switch Is the DHCP Server



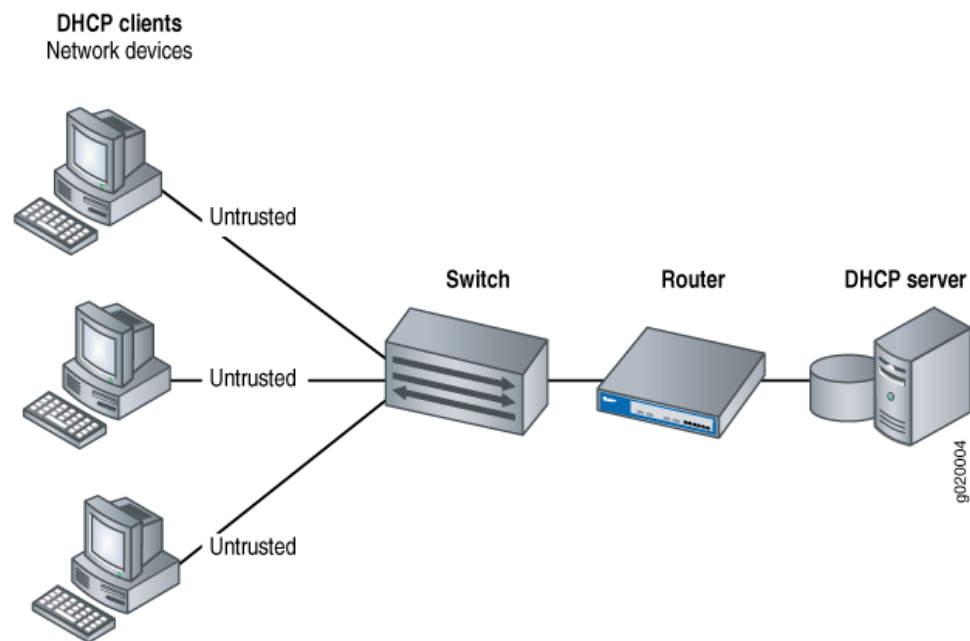
Switch Acts as a Relay Agent

The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface (on a switch or a router). The Layer 3 interfaces on the switch are configured as routed VLAN interfaces (RVIs)—also called integrated routing and bridging (IRB) interfaces. The trunk interfaces are trusted by default.

The switch can act as a relay agent in these two scenarios:

- The DHCP server and clients are in different VLANs.
- The switch is connected to a router that is, in turn, connected to the DHCP server. See [Figure 20 on page 392](#).

Figure 20: Switch Acting as a Relay Agent Through a Router to the DHCP Server



Static IP Address Additions to the DHCP Snooping Database

You can add specific static IP addresses to the database as well as have the addresses dynamically assigned through DHCP snooping. To add a static IP address, you provide the IP address, the MAC address of the device, the interface on which the device is connected, and the VLAN with which the interface is associated. You do not assign a lease time to the entry. The statically configured entry never expires.

Release History Table

Release	Description
14.1X53-D35	Starting in Junos OS Release 14.1X53-D35, a network device with a fixed IP allocation from the DHCP server is replaced by a new device with a different MAC address.
14.1X53-D10	Starting in Junos OS Release 14.1X53-D10, DHCP snooping is supported for IPv6 packets on EX 9200 Switches.
13.2X51-D20	Starting in Junos OS Release 17.1R1, you can configure DHCP snooping or DHCPv6 snooping on a VLAN without enabling other port security features by configuring the dhcp-security CLI statement at the [edit vlans vlan-name forwarding-options dhcp-security] .

Related Documentation

- [Port Security Features on page 3](#)
- [Configuring Port Security \(ELS\) on page 9](#)
- [Understanding and Using Trusted DHCP Servers on page 371](#)
- [DHCP/BOOTP Relay for Switches Overview](#)

- [Configuring Persistent Bindings in the DHCP or DHCPv6 \(ELS\) on page 381](#)
- [Understanding DHCP Option 82 on page 429](#)

Understanding DHCP Snooping (non-ELS)



NOTE: This topic includes information about enabling Dynamic Host Configuration Protocol (DHCP) snooping for Junos EX Series switches that do not support the Enhanced Layer 2 Software (ELS). If your switch runs a version of Junos that supports ELS, see [“Understanding DHCP Snooping \(ELS\)” on page 385](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

DHCP snooping enables the switching device, which can be either a switch or a router, to monitor DHCP messages received from untrusted devices connected to the switching device. When DHCP snooping is enabled on a VLAN, the system examines DHCP messages sent from untrusted hosts associated with the VLAN and extracts their IP addresses and lease information. This information is used to build and maintain the DHCP snooping database. Only hosts that can be verified using this database are allowed access to the network.

- [DHCP Snooping Basics on page 393](#)
- [DHCP Snooping Process on page 394](#)
- [DHCPv6 Snooping on page 395](#)
- [Rapid Commit for DHCPv6 on page 396](#)
- [DHCP Server Access on page 396](#)
- [Static IP Address Additions to the DHCP Snooping Database on page 399](#)
- [Snooping DHCP Packets That Have Invalid IP Addresses on page 399](#)
- [Prioritizing Snooped Packets on page 400](#)

DHCP Snooping Basics

The Dynamic Host Configuration Protocol (DHCP) allocates IP addresses dynamically, *leasing* addresses to devices so that the addresses can be reused when no longer needed. Hosts and end devices that require IP addresses obtained through DHCP must communicate with a DHCP server across the LAN.

DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server (the server is connected to a trusted network port).

By default, all trunk ports on the switch are trusted and all access ports are untrusted for DHCP snooping.

When DHCP snooping is enabled, the lease information from the switching device is used to create the DHCP snooping table, also known as the binding table. The table shows

the IP-MAC binding, as well as the lease time for the IP address, type of binding, VLAN name, and interface for each host.



NOTE: DHCP snooping is disabled in the default configuration of the switching device. You must explicitly enable DHCP snooping by setting `examine-dhcp` at the `[edit ethernet-switching-options secure-access-port]` hierarchy level.

Entries in the DHCP snooping database are updated in these events:

- When a DHCP client releases an IP address (sends a DHCPRELEASE message). In this event, the associated mapping entry is deleted from the database.
- If you move a network device from one VLAN to another. In this event, typically the device needs to acquire a new IP address. Therefore, its entry in the database, including its VLAN ID, is updated.
- When the lease time (timeout value) assigned by the DHCP server expires. In this event, the associated entry is deleted from the database.



TIP: By default, the IP-MAC bindings are lost when the switching device is rebooted and DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the `dhcp-snooping-file` statement to store the database file either locally or remotely.

You can configure the switching device to snoop DHCP server responses from particular VLANs only. This prevents spoofing of DHCP server messages.

You configure DHCP snooping per VLAN, not per interface (port). DHCP snooping is disabled by default on switching devices.

DHCP Snooping Process

The basic process of DHCP snooping consists of the following steps:



NOTE: When DHCP snooping is enabled for a VLAN, all DHCP packets sent from the network devices in that VLAN are subjected to DHCP snooping. The final IP-MAC binding occurs when the DHCP server sends DHCPACK to the DHCP client.

1. The network device sends a DHCPDISCOVER packet to request an IP address.
2. The switching device forwards the packet to the DHCP server.

3. The server sends a DHCPOFFER packet to offer an address. If the DHCPOFFER packet is from a trusted interface, the switching device forwards the packet to the DHCP client.
4. The network device sends a DHCPREQUEST packet to accept the IP address. The switching device adds an IP-MAC placeholder binding to the database. The entry is considered a placeholder until a DHCPACK packet is received from the server. Until then, the IP address could still be assigned to some other host.
5. The server sends a DHCPACK packet to assign the IP address or a DHCPNAK packet to deny the address request.
6. The switching device updates the DHCP snooping database according to the type of packet received:
 - If the switching device receives a DHCPACK packet, it updates lease information for the IP-MAC bindings in its database.
 - If the switching device receives a DHCPNAK packet, it deletes the placeholder.



NOTE: The DHCP snooping database is updated only after the DHCPREQUEST packet has been sent.

For general information about the messages that the DHCP client and DHCP server exchange during the assignment of an IP address for the client, see the *Junos OS Administration Library*.

DHCPv6 Snooping

DHCPv6 snooping is the equivalent of DHCP snooping for IPv6. The process for DHCPv6 snooping is similar to that for DHCP snooping, but uses different names for the messages exchanged between the client and server to assign IPv6 addresses. [Table 21 on page 388](#) shows DHCPv6 messages and their DHCP equivalents.

Table 22: DHCPv6 Messages and Equivalent DHCPv4 Messages

Sent by	DHCPv6 Messages	Equivalent DHCP Messages
Client	SOLICIT	DHCPDISCOVER
Server	ADVERTISE	DHCPOFFER
Client	REQUEST, RENEW, REBIND	DHCPREQUEST
Server	REPLY	DHCPACK/DHCPNAK
Client	RELEASE	DHCPRELEASE
Client	INFORMATION-REQUEST	DHCPINFORM

Table 22: DHCPv6 Messages and Equivalent DHCPv4 Messages (continued)

Sent by	DHCPv6 Messages	Equivalent DHCP Messages
Client	DECLINE	DHCPDECLINE
Client	CONFIRM	none
Server	RECONFIGURE	DHCPFORCERENEW
Client	RELAY-FORW, RELAY-REPLY	none

Rapid Commit for DHCPv6

DHCPv6 provides for a Rapid Commit option (DHCPv6 option 14), which, when supported by the server and set by the client, shortens the exchange from a four-way relay to a two-message handshake. For more information about enabling the Rapid Commit option, see [“Configuring DHCPv6 Rapid Commit \(MX, EX\)” on page 378](#).

In the rapid commit process:

1. The DHCPv6 client sends out a SOLICIT message that contains a request that rapid assignment of address, prefix, and other configuration parameters be preferred.
2. If the DHCPv6 server supports rapid assignment, it responds with a REPLY message, which contains the assigned IPv6 address and prefix and other configuration parameters.

DHCP Server Access

You can configure a switching device’s access to the DHCP server in three ways:

- [Switching Device, DHCP Clients, and DHCP Server Are All on the Same VLAN on page 396](#)
- [Switching Device Acts as DHCP Server on page 397](#)
- [Switching Device Acts as Relay Agent on page 398](#)

Switching Device, DHCP Clients, and DHCP Server Are All on the Same VLAN

When the switching device, DHCP clients, and DHCP server are *all members of the same VLAN*, the DHCP server can be connected to the switching device in one of two ways:

- The server is directly connected to the same switching device as the one connected to the DHCP clients (the hosts, or network devices, that are requesting IP addresses from the server). The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. See [Figure 17 on page 390](#).
- The server is connected to an intermediary switching device (Switching Device 2). The DHCP clients are connected to Switching Device 1, which is connected through a trunk port to Switching Device 2. Switching Device 2 is being used as a transit device. The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk

port is configured by default as a trusted port. As shown in [Figure 18 on page 390](#), ge-0/0/11 is a trusted trunk port.

Figure 21: DHCP Server Connected Directly to a Switching Device

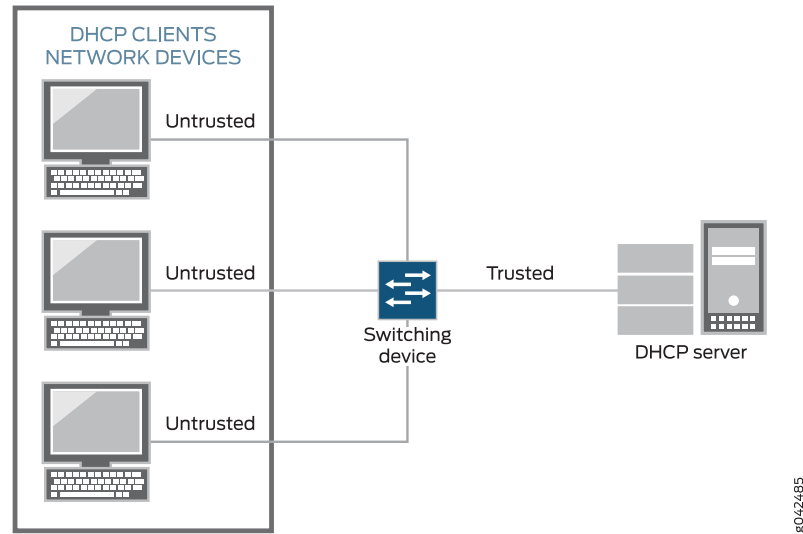
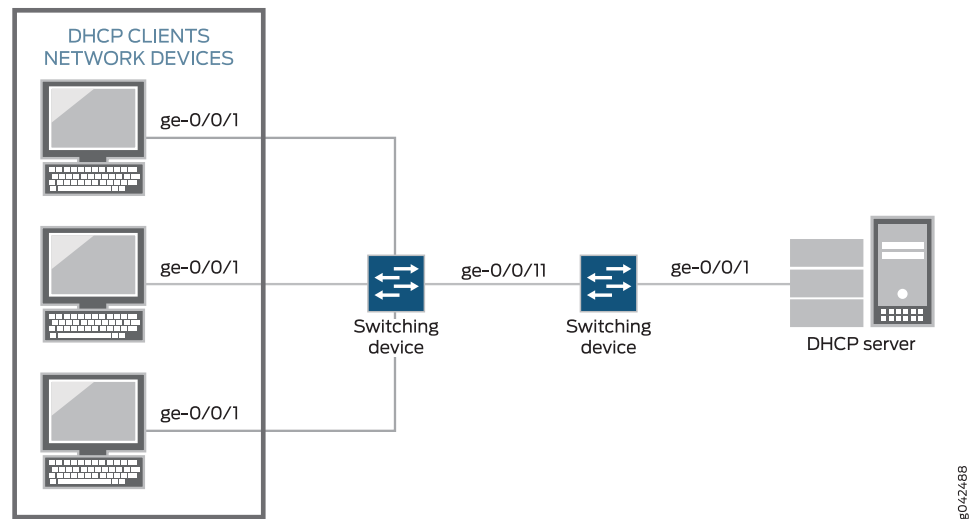


Figure 22: DHCP Server Connected Directly to Switching Device 2, with Switching Device 2 Connected to Switching Device 1 Through a Trusted Trunk Port



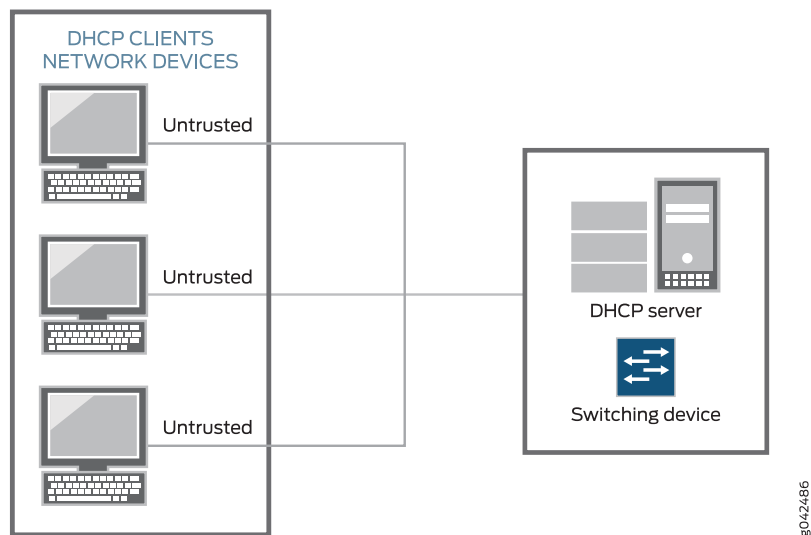
Switching Device Acts as DHCP Server



NOTE: The switching device acting as a DHCP server is not supported on the QFX Series.

The switching device itself is configured as a DHCP server; this is known as a *local configuration*. See [Figure 19 on page 391](#).

Figure 23: Switching Device Is the DHCP Server



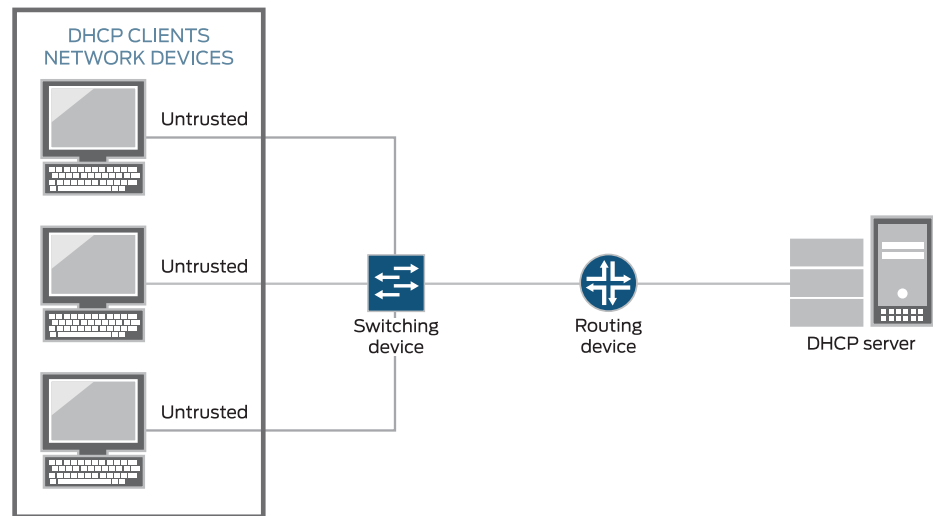
Switching Device Acts as Relay Agent

The switching device functions as a relay agent when the DHCP clients or the DHCP server is connected to the device through a Layer 3 interface. The Layer 3 interfaces on the switching device are configured as routed VLAN interfaces (RVIs), which are also known as integrated routing and bridging (IRB) interfaces. The trunk interfaces are trusted by default.

These two scenarios illustrate the switching device acting as a relay agent:

- The DHCP server and clients are in different VLANs.
- The switching device is connected to a router that is in turn connected to the DHCP server. See [Figure 20 on page 392](#).

Figure 24: Switching Device Acting as Relay Agent Through Router to DHCP Server



8042487

Static IP Address Additions to the DHCP Snooping Database

You can add specific static IP addresses to the database as well as have the addresses dynamically assigned through DHCP snooping. To add static IP addresses, you supply the IP address, the MAC address of the device, the interface on which the device is connected, and the VLAN with which the interface is associated. No lease time is assigned to the entry. The statically configured entry never expires.

Snooping DHCP Packets That Have Invalid IP Addresses

If you enable DHCP snooping on a VLAN and then devices on that VLAN send DHCP packets that request invalid IP addresses, these invalid IP addresses are stored in the DHCP snooping database until they are deleted when their default timeout is reached. To eliminate this unnecessary consumption of space in the DHCP snooping database, the switching device drops the DHCP packets that request invalid IP addresses, preventing the snooping of these packets. The invalid IP addresses are:

- 0.0.0.0
- 128.0.x.x
- 191.255.x.x
- 192.0.0.x
- 223.255.255.x
- 224.x.x.x
- 240.x.x.x to 255.255.255.255

Prioritizing Snooped Packets



NOTE: Prioritizing snooped packets is not supported on the QFX Series and the EX4600 switch.

You can use class-of-service (CoS) forwarding classes and queues to prioritize DHCP snooped packets for a specified VLAN. This type of configuration places the DHCP snooped packets for that VLAN in a specified egress queue, so that the security procedure does not interfere with the transmission of high-priority traffic.

Related Documentation

- [Port Security Features on page 3](#)
- [Understanding and Using Trusted DHCP Servers on page 371](#)
- [Configuring Static DHCP IP Addresses for DHCP snooping \(MX routers\) on page 406](#)

Enabling DHCP Snooping (non-ELS)

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. The switch builds and maintains a database of valid bindings between IP address and MAC addresses (IP-MAC bindings) called the DHCP snooping database.



NOTE: If you configure DHCP snooping for all VLANs and you enable a different port security feature on a specific VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

- [Enabling DHCP Snooping on page 401](#)
- [Applying CoS Forwarding Classes to Prioritize Snooped Packets on page 401](#)
- [Verifying That DHCP Snooping Is Working Correctly on page 402](#)

Enabling DHCP Snooping

You configure DHCP snooping per VLAN, not per interface (port). By default, DHCP snooping is disabled for all VLANs. You can enable DHCP snooping on all VLANs or on specific VLANs.

To enable DHCP snooping:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan vlan-name examine-dhcp
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all examine-dhcp
```

To enable DHCPv6 snooping:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan vlan-name examine-dhcpv6
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all examine-dhcpv6
```



TIP: By default, the IP-MAC bindings are lost when the switch is rebooted and DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the switch to store the database file either locally or remotely. See [“Configuring Persistent Bindings in the DHCP or DHCPv6 \(non-ELS\)”](#) on page 383.



TIP: For private VLANs (PVLANS), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from PVLAN trunk ports are not snooped.

Applying CoS Forwarding Classes to Prioritize Snooped Packets

On EX Series switches you might need to use class of service (CoS) to protect packets from critical applications from being dropped during periods of network congestion and delay, and might also need to configure the port security features of DHCP snooping on the ports through which those packets enter or leave.



NOTE: Prioritizing snooped packets by using CoS forwarding classes is not supported on the QFX Series switch.

To apply CoS forwarding classes and queues to snooped packets:

1. Create a user-defined forwarding class to be used for prioritizing snooped packets:

```
[edit class-of-service]
user@switch# set forwarding-classes class class-name queue-num queue-number
```

2. Enable DHCP snooping on a specific VLAN or on all VLANs and apply the required forwarding class on the snooped packets:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan vlan-name examine-dhcp forwarding-class class-name
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all examine-dhcp forwarding-class class-name
```



NOTE: Replace `examine-dhcp` with `examine-dhcpv6` to enable DHCPv6 snooping.

Verifying That DHCP Snooping Is Working Correctly

Purpose Verify that DHCP snooping is working on the switch and that the DHCP snooping database is correctly populated with both dynamic and static bindings.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp snooping binding
```

```
DHCP Snooping Information:
MAC address      IP address  Lease (seconds) Type      VLAN      Interface
00:05:85:3A:82:77 192.0.2.17  600          dynamic employee ge-0/0/1.0
00:05:85:3A:82:79 192.0.2.18  653          dynamic employee ge-0/0/1.0
00:05:85:3A:82:80 192.0.2.19  720          dynamic employee ge-0/0/2.0
00:05:85:3A:82:81 192.0.2.20  932          dynamic employee ge-0/0/2.0
00:05:85:3A:82:83 192.0.2.21  1230         dynamic employee ge-0/0/2.0
00:05:85:27:32:88 192.0.2.22  -            static   data      ge-0/0/4.0
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires. Static IP addresses have no assigned lease time. The statically configured entry never expires.

If the DHCP server had been configured as untrusted, no entries would be added to the DHCP snooping database and nothing would be shown in the output of the **show dhcp snooping binding** command.

- Related Documentation**
- [Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks on page 406](#)
 - [Example: Protecting Against ARP Spoofing Attacks on page 418](#)
 - [Example: Prioritizing Snooped and Inspected Packet on page 423](#)
 - [Monitoring Port Security](#)
 - [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

Configuring Static DHCP IP Addresses

- [Configuring Static DHCP IP Addresses for DHCP snooping \(ELS\) on page 404](#)
- [Configuring Static DHCP IP Addresses for DHCP snooping \(non-ELS\) on page 405](#)
- [Configuring Static DHCP IP Addresses for DHCP snooping \(MX routers\) on page 406](#)

Configuring Static DHCP IP Addresses for DHCP snooping (ELS)



NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see [“Configuring Static DHCP IP Addresses for DHCP snooping \(non-ELS\)”](#) on page 405. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

You can add static (fixed) IP addresses and bind them to fixed MAC addresses in the DHCP snooping database. These bindings are labeled *static* in the database, while those bindings that have been added through the process of DHCP snooping are labeled *dynamic*. Static IPv6 address assignment is also available for DHCPv6.

Before you can perform this procedure, you must configure the VLAN. See *Configuring VLANs for EX Series Switches with ELS Support (CLI Procedure)*.

To configure a static IP address to MAC address (IP-MAC) binding in the DHCP snooping database, you must first create a group of access interfaces under the **[edit vlans vlan-name forwarding-options dhcp-security]** hierarchy. Creating this group automatically enables DHCP snooping, which is a prerequisite for creating the DHCP snooping database. You can then configure a specific interface within the group to have a static IP address that is bound to a fixed MAC address. If you want to have multiple static IP addresses, configure additional interfaces within the same group.



NOTE: On switches that support DHCPv6, creating the group of interfaces will automatically enable both DHCP and DHCPv6 snooping.

To configure a static IP-MAC address binding in the DHCP snooping database:

- [edit vlans vlan-name forwarding-options dhcp-security]
user@switch# **set group group-name interface interface-name static-ip ip-address mac mac-address**

To configure a static IPv6-MAC address binding in the DHCPv6 snooping database:

- [edit vlans vlan-name forwarding-options dhcp-security]
user@switch# **set group group-name interface interface-name static-ipv6 ip-address mac mac-address**

In the following example, a device with static IP allocation is connected to the ge-0/0/1 interface, which belongs to vlan-A. To configure this device to connect to the external network:

```
[edit]
user@switch# set vlans vlan-A forwarding-options dhcp-security group static-group interface
ge-0/0/1 static-ip 10.1.1.6 mac 00:00:00:44:44:06
```

To verify that the configuration is configured on the device:


```

user@switch> show configuration vlans vlan-A
vlan-id 100;
forwarding-options {
  dhcp-security {
    ip-source-guard;
    group static-group {
      interface ge-0/0/1 {
        static-ip 10.1.1.6 mac 00:00:00:44:44:06
      }
    }
  }
}

```

To verify that a binding entry is created for the static client:

```
user@switch> show dhcp-security binding
```

IP address	MAC address	Vlan	Expires	State	Interface
10.1.1.6	00:00:00:44:44:06	vlan-A	0	STATIC	ge-0/0/1

- See Also**
- [show dhcp-security binding on page 1183](#)
 - [Enabling DHCP Snooping \(non-ELS\) on page 400](#)
 - [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

Configuring Static DHCP IP Addresses for DHCP snooping (non-ELS)

You can add static (fixed) IP addresses and bind them to fixed MAC addresses in the DHCP snooping database. These bindings are labeled *static* in the database, while those bindings that have been added through the process of DHCP snooping are labeled *dynamic*.



NOTE: This task uses Junos OS for EX Series switches that do not support Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does support ELS, see [“Configuring Static DHCP IP Addresses for DHCP snooping \(ELS\)” on page 404](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

To configure a static IP-MAC address binding in the DHCP snooping database:

```

[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name static-ip ip-address vlan data-vlan mac mac-address

```

To configure a static IP-MAC address binding in the DHCPv6 snooping database:

```

[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name static-ipv6 ip-address vlan data-vlan mac mac-address

```

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

- See Also**
- [Enabling DHCP Snooping \(non-ELS\) on page 400](#)
 - [Understanding DHCP Snooping \(non-ELS\) on page 393](#)
 - [secure-access-port on page 979](#)
 - *secure-access-port*

Configuring Static DHCP IP Addresses for DHCP snooping (MX routers)

You can add static (fixed) IP addresses and bind them to fixed MAC addresses in the DHCP snooping database. These bindings are labeled as *static* in the database, while those bindings that have been added through the process of DHCP snooping are labeled *dynamic*.

To configure a static IP address/MAC address binding in the DHCP snooping database, you must first create a group of access interfaces under **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]**. Creating this group automatically enables DHCP snooping, which is a prerequisite for creating the DHCP snooping database. The following procedure shows the configuration in two steps, but it can be done in one. You can then configure a specific interface within the group to have a static IP address that is bound to a fixed MAC address. If you want to have multiple static IP addresses, configure additional interfaces within the same group.

To configure a static IP address and MAC address binding in the DHCP snooping database:

1. Create a group by including an access interface:

```
[edit bridge-domains bd-name forwarding-options dhcp-security]
user@device# set group group-name interface interface-name
```

2. Configure a static IP address:

```
[edit bridge-domains bd-name forwarding-options dhcp-security]
user@device# set group group-name interface interface-name static-ip ip-address
mac mac-address
```

- See Also**
- [show dhcp-security binding on page 1183](#)
 - [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks

You can configure DHCP snooping, dynamic ARP inspection (DAI), and MAC limiting on the access interfaces of a switch to protect the switch and the Ethernet LAN against address spoofing and Layer 2 denial-of-service (DoS) attacks. To obtain the basic settings for these features, you can use the switch's default configuration for port security,

configure the MAC limit, and enable DHCP snooping and DAI on a VLAN. You can configure these features when the DHCP server is connected to a switch that is different from the one to which the DHCP clients (network devices) are connected.

This example describes how to configure port security features on a switch whose hosts obtain IP addresses and lease times from a DHCP server connected to a second switch:

- [Requirements on page 407](#)
- [Overview and Topology on page 407](#)
- [Configuring a VLAN, Interfaces, and Port Security Features on Switch 1 on page 409](#)
- [Configuring a VLAN and Interfaces on Switch 2 on page 411](#)
- [Verification on page 413](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch or QFX3500 switch—*Switch 1* in this example.
- An additional EX Series switch or QFX3500 switch—*Switch 2* in this example. You do not configure port security on this second switch.
- Junos OS Release 9.0 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series.
- A DHCP server connected to Switch 2. You use the server to provide IP addresses to network devices connected to Switch 1.
- At least two network devices (hosts) that you connect to access interfaces on Switch 1. These devices are DHCP clients.

Before you configure DHCP snooping, DAI, and MAC limiting port security features, be sure you have:

- Connected the DHCP server to Switch 2.
- Configured a VLAN on Switch 1. See the task for your platform:
 - *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
 - *Example: Setting Up Bridging with Multiple VLANs for the QFX Series*

Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. To protect the devices from such attacks, you can configure:

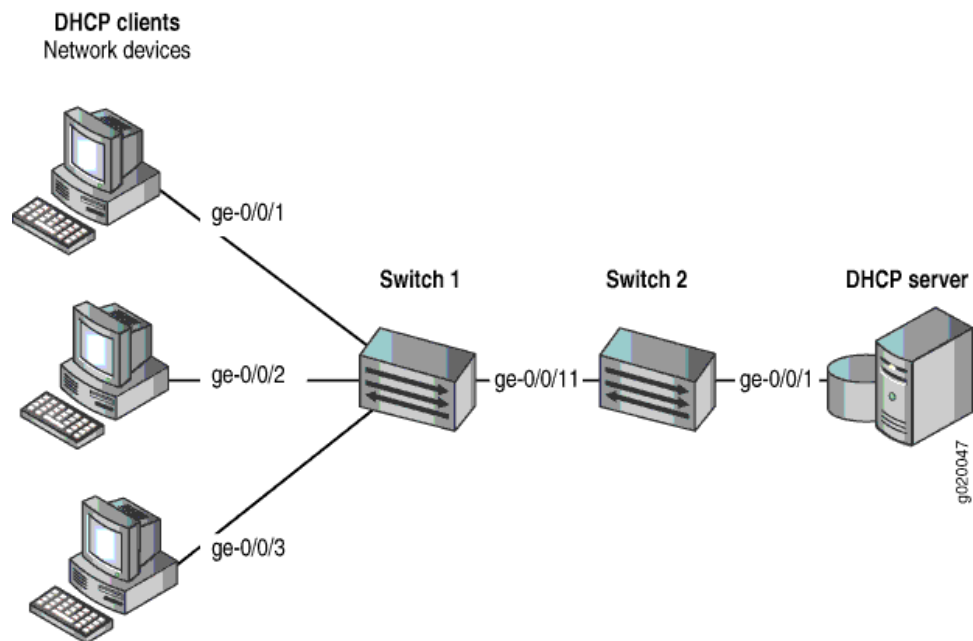
- DHCP snooping to validate DHCP server messages
- DAI to protect against ARP spoofing
- MAC limiting to constrain the number of MAC addresses the switch adds to its MAC address cache

This example shows how to configure these port security features on Switch 1. Switch 1 is connected to another switch (Switch 2), which is not configured with port security features. Switch 2 is connected to a DHCP server (see [Figure 25 on page 408](#).) Network devices (hosts) that are connected to Switch 1 send requests for IP addresses (these network devices are DHCP clients). Those requests are transmitted from Switch 1 to Switch 2 and then to the DHCP server connected to Switch 2. Responses to the requests are transmitted along the reverse path of the one followed by the requests.

The setup for this example includes the VLAN **employee-vlan** on both switches.

[Figure 25 on page 408](#) shows the network topology for the example.

Figure 25: Network Topology for Port Security Setup with Two Switches on the Same VLAN



The components of the topology for this example are shown in [Table 23 on page 408](#).

Table 23: Components of Port Security Setup on Switch 1 with a DHCP Server Connected to Switch 2

Properties	Settings
Switch hardware	One EX Series switch or one QFX3500 switch (Switch 1), and an additional EX Series switch or QFX3500 switch (Switch 2)
VLAN name and ID	employee-vlan, tag 20
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is subnet's broadcast address
Trunk interface on both switches	ge-0/0/11
Access interfaces on Switch 1	ge-0/0/1, ge-0/0/2, and ge-0/0/3

Table 23: Components of Port Security Setup on Switch 1 with a DHCP Server Connected to Switch 2 (continued)

Properties	Settings
Access interface on Switch 2	ge-0/0/1
Interface for DHCP server	ge-0/0/1 on Switch 2

Switch 1 is initially configured with the default port security setup. In the default configuration on the switch:

- Secure port access is activated on the switch.
- The switch does not drop any packets, which is the default setting.
- DHCP snooping and DAI are disabled on all VLANs.
- All access interfaces are untrusted and trunk interfaces are trusted; these are the default settings.

In the configuration tasks for this example, you configure a VLAN on both switches.

In addition to configuring the VLAN, you enable DHCP snooping on Switch 1. In this example, you also enable DAI and a MAC limit of 5 on Switch 1.

Because the interface that connects Switch 2 to Switch 1 is a trunk interface, you do not need to configure this interface to be trusted. As noted above, trunk interfaces are automatically trusted, so DHCP messages coming from the DHCP server to Switch 2 and then on to Switch 1 are trusted.

Configuring a VLAN, Interfaces, and Port Security Features on Switch 1

CLI Quick Configuration To quickly configure a VLAN, interfaces, and port security features, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans employee-vlan vlan-id 20
set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members 20
set ethernet-switching-options secure-access-port interface ge-0/0/1 mac-limit 5 action drop
set ethernet-switching-options secure-access-port vlan employee-vlan arp-inspection
set ethernet-switching-options secure-access-port vlan employee-vlan examine-dhcp
clear ethernet-switching table interface ge-0/0/1
```

Step-by-Step Procedure To configure MAC limiting, a VLAN, and interfaces on Switch 1 and enable DAI and DHCP on the VLAN:

1. Configure the VLAN **employee-vlan** with VLAN ID **20**:

```
[edit vlans]
user@switch1# set employee-vlan vlan-id 20
```

2. Configure an interface on Switch 1 as a trunk interface:

```
[edit interfaces]
user@switch1# set ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
```

3. Associate the VLAN with interfaces ge-0/0/1, ge-0/0/2, ge-0/0/3, and ge-0/0/11:

```
[edit interfaces]
user@switch1# set ge-0/0/1 unit 0 family ethernet-switching vlan members 20
user@switch1# set ge-0/0/2 unit 0 family ethernet-switching vlan members 20
user@switch1# set ge-0/0/3 unit 0 family ethernet-switching vlan members 20
user@switch1# set ge-0/0/11 unit 0 family ethernet-switching vlan members 20
```

4. Enable DHCP snooping on the VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch1# set vlan employee-vlan examine-dhcp
```

5. Enable DAI on the VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch1# set vlan employee-vlan arp-inspection
```

6. Configure a MAC limit of **5** on ge-0/0/1 and use the default action, **drop** (packets with new addresses are dropped if the limit is exceeded):

```
[edit ethernet-switching-options secure-access-port]
user@switch1# set interface ge-0/0/1 mac-limit 5 drop
```

7. Clear the existing MAC address table entries from interface ge-0/0/1:

```
user@switch1# clear ethernet-switching table interface ge-0/0/1
```

Results Display the results of the configuration:

```
[edit]
user@switch1# show
ethernet-switching-options {
  secure-access-port {
    interface ge-0/0/1.0 {
      mac-limit 5 action drop;
    }
  }
  vlan employee-vlan {
    arp-inspection;
    examine-dhcp;
  }
}
```

```

    }
  }
}
interfaces {
  ge-0/0/1 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members 20;
        }
      }
    }
  }
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members 20;
        }
      }
    }
  }
  ge-0/0/3 {
    unit 0 {
      family ethernet-switching {
        vlan {
          port-mode trunk;
          members 20;
        }
      }
    }
  }
  ge-0/0/11 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 20;
        }
      }
    }
  }
}
vlans {
  employee-vlan {
    vlan-id 20;
  }
}

```

Configuring a VLAN and Interfaces on Switch 2

To configure the VLAN and interfaces on Switch 2:

CLI Quick Configuration To quickly configure the VLAN and interfaces on Switch 2, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans employee-vlan vlan-id 20
set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members 20
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members 20
```

Step-by-Step Procedure To configure the VLAN and interfaces on Switch 2:

1. Configure the VLAN **employee-vlan** with VLAN ID **20**:

```
[edit vlans]
user@switch1# set employee-vlan vlan-id 20
```

2. Configure an interface on Switch 2 as a trunk interface:

```
[edit interfaces]
user@switch2# set ge-0/0/11 unit 0 ethernet-switching port-mode trunk
```

3. Associate the VLAN with interfaces ge-0/0/1 and ge-0/0/11:

```
[edit interfaces]
user@switch2# set ge-0/0/1 unit 0 family ethernet-switching vlan members 20
user@switch2# set ge-0/0/11 unit 0 family ethernet-switching vlan members 20
```

Results Display the results of the configuration:

```
[edit]
user@switch2# show
interfaces {
  ge-0/0/1 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members 20;
        }
      }
    }
  }
  ge-0/0/11 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 20;
        }
      }
    }
  }
}
vlans {
```



```

employee-vlan {
  vlan-id 20;
}
}

```

Verification

To confirm that the configuration is working properly.

- [Verifying That DHCP Snooping Is Working Correctly on Switch 1 on page 413](#)
- [Verifying That DAI Is Working Correctly on Switch 1 on page 413](#)
- [Verifying That MAC Limiting Is Working Correctly on Switch 1 on page 414](#)

Verifying That DHCP Snooping Is Working Correctly on Switch 1

Purpose Verify that DHCP snooping is working on Switch 1.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

issue the operational mode command **show dhcp snooping binding** to display the DHCP snooping information when the interface through which Switch 2 sends the DHCP server replies to clients connected to Switch 1 is trusted. The server has provided the IP addresses and leases:

```
user@switch1> show dhcp snooping binding
```

DHCP Snooping Information:

MAC Address	IP Address	Lease	Type	VLAN	Interface
00:05:85:3A:82:77	192.0.2.17	600	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:79	192.0.2.18	653	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:80	192.0.2.19	720	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:81	192.0.2.20	932	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:83	192.0.2.21	1230	dynamic	employee-vlan	ge-0/0/1.0
00:05:85:3A:82:90	192.0.2.20	932	dynamic	employee-vlan	ge-0/0/2.0
00:05:85:3A:82:91	192.0.2.21	1230	dynamic	employee-vlan	ge-0/0/3.0

Meaning The output shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

Verifying That DAI Is Working Correctly on Switch 1

Purpose Verify that DAI is working on Switch 1.

Action Send some ARP requests from network devices connected to the switch.

Issue the operational mode command **show arp inspection statistics** to display the DAI information:

```
user@switch1> show arp inspection statistics
```

ARP inspection statistics:

Interface	Packets received	ARP inspection pass	ARP inspection failed
ge-0/0/1.0	7	5	2
ge-0/0/2.0	10	10	0
ge-0/0/3.0	18	15	3

Meaning The output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

Verifying That MAC Limiting Is Working Correctly on Switch 1

Purpose Verify that MAC limiting is working on Switch 1.

Action Issue the operational mode command **show ethernet-switching table** to display the MAC addresses that are learned when DHCP requests are sent from hosts on ge-0/0/1:

```
user@switch1> show ethernet-switching table
```

Ethernet-switching table: 6 entries, 5 learned

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	00:05:85:3A:82:77	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:79	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/1.0
employee-vlan	*	Flood	-	ge-0/0/1.0

Meaning The output shows that five MAC addresses have been learned for interface **ge-0/0/1**, which corresponds to the MAC limit of **5** set in the configuration. The last line of the output shows that a sixth MAC address request was dropped, as indicated by the asterisk (*) in the **MAC address** column.

Related Documentation

- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Configuring Port Security \(non-ELS\) on page 11](#)

- *Configuring Port Security (J-Web Procedure)*
- [secure-access-port on page 979](#)
- *secure-access-port*
- [show arp inspection statistics on page 1130](#)
- [show dhcp snooping binding on page 1178](#)
- [show ethernet-switching table on page 1198](#)

Example: Protecting Against DHCP Snooping Database Attacks

In one type of attack on the DHCP snooping database, an intruder introduces a DHCP client on an untrusted access interface with a MAC address identical to that of a client on another untrusted interface. The intruder then acquires the DHCP lease of that other client, thus changing the entries in the DHCP snooping table. Subsequently, what would have been valid ARP requests from the legitimate client are blocked.

This example describes how to configure allowed MAC addresses, a port security feature, to protect the switch from DHCP snooping database alteration attacks:

- [Requirements on page 415](#)
- [Overview and Topology on page 416](#)
- [Configuration on page 417](#)
- [Verification on page 417](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch or one QFX3500 switch
- Junos OS Release 11.4 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure specific port security features to mitigate common access-interface attacks, be sure you have:

- Connected the DHCP server to the switch.
- Configured a VLAN on the switch. See the task for your platform:
 - *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
 - *Example: Setting Up Bridging with Multiple VLANs for the QFX Series*

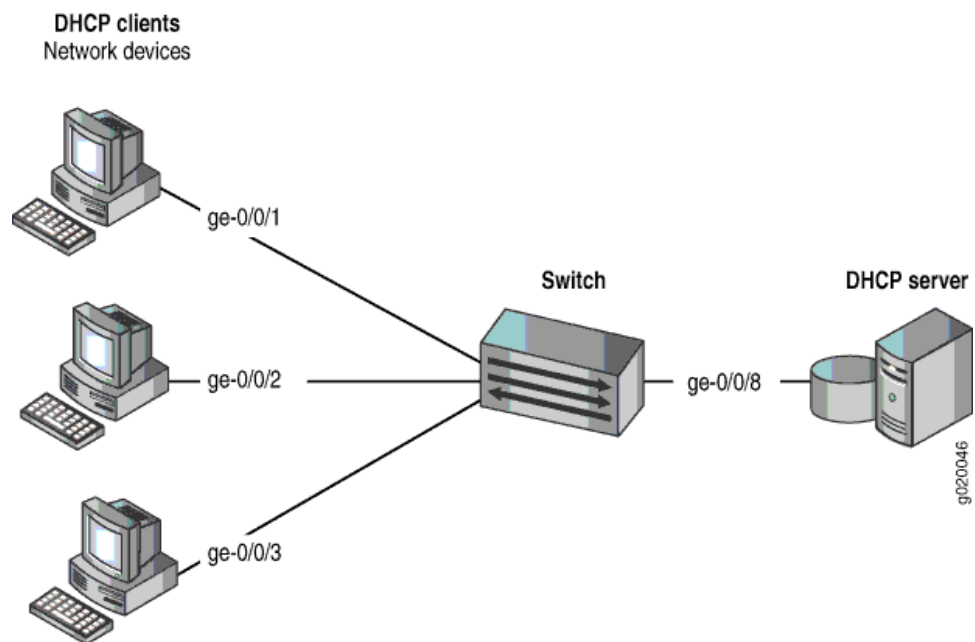
Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch from an attack on the DHCP snooping database that alters the MAC addresses assigned to some clients.

This example shows how to configure port security features on a switch that is connected to a DHCP server.

The setup for this example includes the VLAN **employee-vlan** on the switch. [Figure 26 on page 416](#) illustrates the topology for this example.

Figure 26: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 24 on page 416](#).

Table 24: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	employee-vlan , tag 20
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is the subnet's broadcast address
Interfaces in employee-vlan	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface for DHCP server	ge-0/0/8

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- DHCP snooping is enabled on the VLAN **employee-vlan**.
- All access ports are untrusted, which is the default setting.

Configuration

To configure allowed MAC addresses to protect the switch against DHCP snooping database alteration attacks:

CLI Quick Configuration To quickly configure some allowed MAC addresses on an interface, copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88
```

Step-by-Step Procedure To configure some allowed MAC addresses on an interface:

Configure the five allowed MAC addresses on an interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:85
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:88
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/2.0 {
  allowed-mac [ 00:05:85:3a:82:80 00:05:85:3a:82:81 00:05:85:3a:82:83 00:05:85:3a:82:85 00:05:85:3a:82:88 ];
}
```

Verification

Confirm that the configuration is working properly.

- [Verifying That Allowed MAC Addresses Are Working Correctly on the Switch on page 417](#)

Verifying That Allowed MAC Addresses Are Working Correctly on the Switch

Purpose Verify that allowed MAC addresses are working on the switch.

Action Display the MAC cache information:

```
user@switch> show ethernet-switching table
```

```
Ethernet-switching table: 6 entries, 5 learned
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:88	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

Meaning The output shows that the five MAC addresses configured as allowed MAC addresses have been learned and are displayed in the MAC cache. The last MAC address in the list, one that had not been configured as allowed, has not been added to the list of learned addresses.

Related Documentation

- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Configuring MAC Limiting \(non-ELS\) on page 341](#)

Example: Protecting Against ARP Spoofing Attacks

In an ARP spoofing attack, the attacker associates its own MAC address with the IP address of a network device connected to the switch. Traffic intended for that IP address is now sent to the attacker instead of being sent to the intended destination. The attacker can send faked, or “spoofed,” ARP messages on the LAN.



NOTE: When dynamic ARP inspection (DAI) is enabled, the switch logs the number of invalid ARP packets that it receives on each interface, along with the sender’s IP and MAC addresses. You can use these log messages to discover ARP spoofing on the network. ARP probe packets are not subjected to dynamic ARP inspection. The switch always forwards such packets.

This example describes how to configure DHCP snooping and dynamic ARP inspection (DAI), two port security features, to protect the switch against ARP spoofing attacks:

- [Requirements on page 419](#)
- [Overview and Topology on page 419](#)
- [Configuration on page 420](#)
- [Verification on page 421](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch or one QFX3500 switch
- Junos OS Release 11.4 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure DHCP snooping and DAI (two port security features) to mitigate ARP spoofing attacks, be sure you have:

- Connected the DHCP server to the switch.
- Configured a VLAN on the switch. See the task for your platform:
 - *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
 - *Example: Setting Up Bridging with Multiple VLANs on Switches for QFX Series Switches*

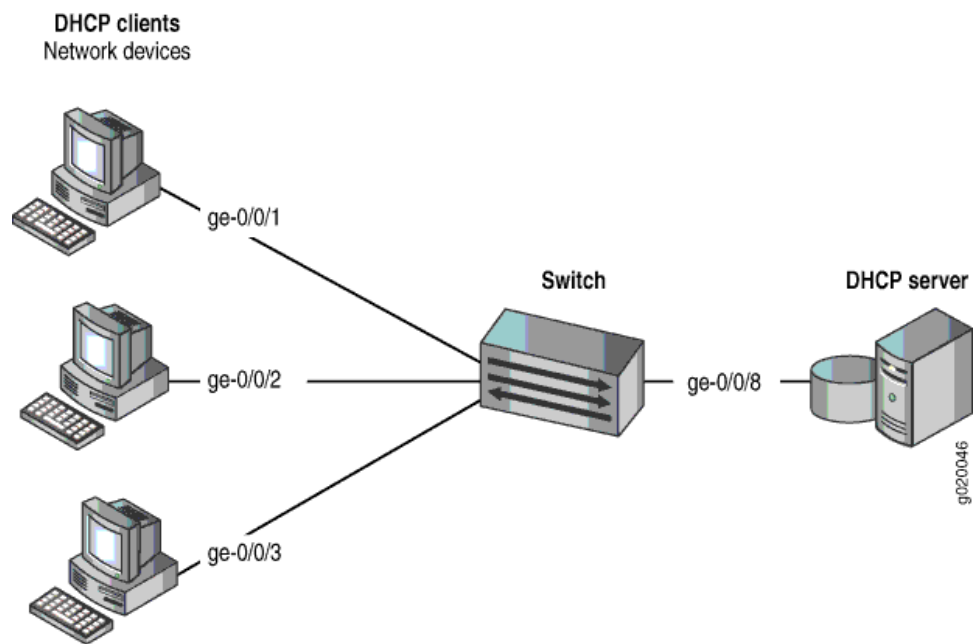
Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. This example describes how to protect the switch against one common type of attack, an ARP spoofing attack.

In an ARP spoofing attack, the attacker sends faked ARP messages, thus creating various types of problems on the LAN—for example, the attacker might launch a man-in-the middle attack.

This example shows how to configure port security features on a switch that is connected to a DHCP server. The setup for this example includes the VLAN **employee-vlan** on the switch. The procedure for creating that VLAN is described in the topic *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches* and *Example: Setting Up Bridging with Multiple VLANs on Switches* for the QFX Series. That procedure is not repeated here. [Figure 27 on page 420](#) illustrates the topology for this example.

Figure 27: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 25 on page 420](#).

Table 25: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX3200-24P, 24 ports (8 PoE ports) or one QFX3500 switch
VLAN name and ID	employee-vlan , tag 20
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is the subnet's broadcast address
Interfaces in employee-vlan	<code>ge-0/0/1</code> , <code>ge-0/0/2</code> , <code>ge-0/0/3</code> , <code>ge-0/0/8</code>
Interface for DHCP server	<code>ge-0/0/8</code>

In this example, the switch has already been configured as follows:

- Secure port access is activated on the switch.
- DHCP snooping is disabled on the VLAN **employee-vlan**.
- All access ports are untrusted, which is the default setting.

Configuration

To configure DHCP snooping and dynamic ARP inspection (DAI) to protect the switch against ARP attacks:

CLI Quick Configuration To quickly configure DHCP snooping and dynamic ARP inspection (DAI), copy the following commands and paste them into the switch terminal window:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/8 dhcp-trusted
user@switch# set vlan employee-vlan examine-dhcp
user@switch# set vlan employee-vlan arp-inspection
```

Step-by-Step Procedure Configure DHCP snooping and dynamic ARP inspection (DAI) on the VLAN:

1. Set the **ge-0/0/8** interface as trusted:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface ge-0/0/8 dhcp-trusted
```

2. Enable DHCP snooping on the VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan examine-dhcp
```

3. Enable DAI on the VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan arp-inspection
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
interface ge-0/0/8.0 {
  dhcp-trusted;
}
vlan employee-vlan {
  arp-inspection;
  examine-dhcp;
}
```

Verification

Confirm that the configuration is working properly.

- [Verifying That DHCP Snooping Is Working Correctly on the Switch on page 421](#)
- [Verifying That DAI Is Working Correctly on the Switch on page 422](#)

Verifying That DHCP Snooping Is Working Correctly on the Switch

Purpose Verify that DHCP snooping is working on the switch.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the port on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp-snooping binding
```

```
DHCP Snooping Information:
MAC Address      IP Address      Lease      Type      VLAN      Interface
-----
00:05:85:3A:82:77 192.0.2.17      600      dynamic  employee-vlan ge-0/0/1.0
00:05:85:3A:82:79 192.0.2.18      653      dynamic  employee-vlan ge-0/0/1.0
00:05:85:3A:82:80 192.0.2.19      720      dynamic  employee-vlan ge-0/0/2.0
00:05:85:3A:82:81 192.0.2.20      932      dynamic  employee-vlan ge-0/0/2.0
00:05:85:3A:82:83 192.0.2.21      1230     dynamic  employee-vlan ge-0/0/2.0
00:05:85:27:32:88 192.0.2.22      3200     dynamic  employee-vlan ge-0/0/3.0
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

Verifying That DAI Is Working Correctly on the Switch

Purpose Verify that DAI is working on the switch.

Action Send some ARP requests from network devices connected to the switch.

Display the DAI information:

```
user@switch> show arp inspection statistics
```

```
ARP inspection statistics:
Interface      Packets received  ARP inspection pass  ARP inspection failed
-----
ge-0/0/1.0      7                  5                    2
ge-0/0/2.0     10                 10                   0
ge-0/0/3.0     12                 12                   0
```

Meaning The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

- Related Documentation**
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [Enabling DHCP Snooping \(non-ELS\) on page 400](#)
 - [Enabling DHCP Snooping \(J-Web Procedure\)](#)
 - [Enabling Dynamic ARP Inspection \(non-ELS\) on page 452](#)
 - [Enabling Dynamic ARP Inspection \(J-Web Procedure\)](#)
 - [secure-access-port on page 979](#)
 - [show arp inspection statistics on page 1130](#)
 - [show dhcp snooping binding on page 1178](#)

Example: Prioritizing Snooped and Inspected Packet

On EX Series switches you might need to use class of service (CoS) to protect packets from critical applications from being dropped during periods of network congestion and delay and you might also need the port security features of DHCP snooping and dynamic ARP inspection (DAI) on the same ports through which those critical packets are entering and leaving. You can combine the advantages of both these features by using CoS forwarding classes and queues to prioritize snooped and inspected packets. This type of configuration places the snooped and inspected packets in the desired egress queue, ensuring that the security procedure does not interfere with the transmittal of this high-priority traffic. This is especially important for traffic that is sensitive to jitter and delay, such as voice traffic.

This example shows how to configure the switch to prioritize snooped and inspected packets in heavy network traffic.

- [Requirements on page 423](#)
- [Overview and Topology on page 424](#)
- [Configuration on page 425](#)
- [Verification on page 426](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 11.2 or later for EX Series switches
- A DHCP server to provide IP addresses to network devices on the switch

Before you specify CoS forwarding classes for snooped and inspected packets, be sure you have:

- Connected the DHCP server to the switch.
- Configured the VLAN **VLAN200** on the switch. See *Configuring VLANs for EX Series Switches*.

- Configured two interfaces, **ge-0/0/1** and **ge-0/0/8**, to belong to **VLAN200**.

Overview and Topology

Ethernet LANs are vulnerable to address spoofing and DoS attacks on network devices. To protect the devices from such attacks, you can configure DHCP snooping to validate DHCP server messages and DAI to protect against MAC spoofing. If you have to deal with periods of heavy network congestion and you want to ensure that sensitive traffic is not disrupted, you can combine the port security features with CoS forwarding classes to prioritize the handling of the snooped and inspected security packets.

In the default switch configuration:

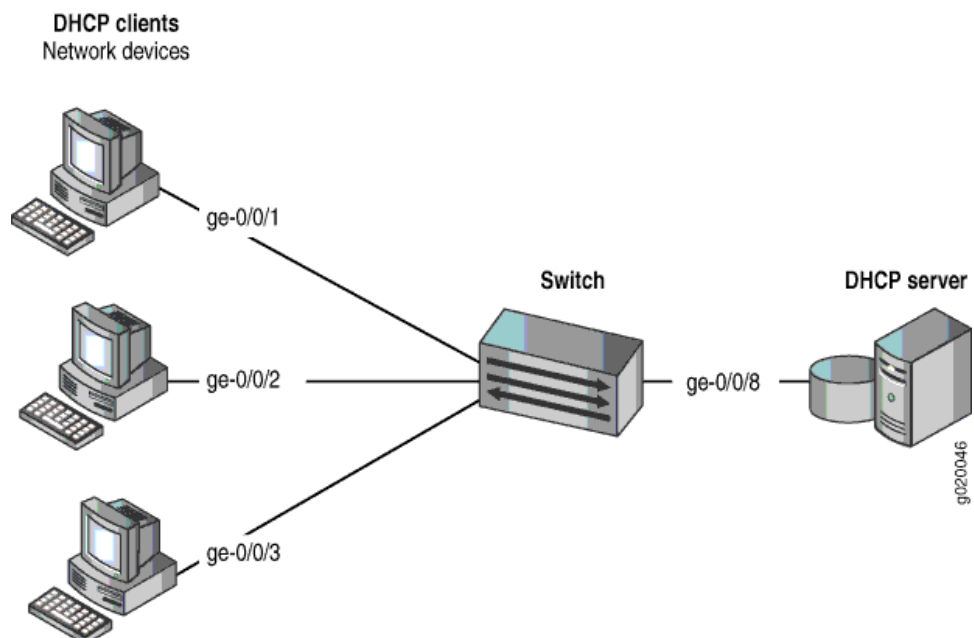
- Secure port access is activated on the switch.
- DHCP snooping and DAI are disabled on all VLANs.
- All access ports are untrusted and all trunk ports are trusted for DHCP snooping.

This example shows how to combine the DHCP snooping and DAI security features with prioritized forwarding of snooped and inspected packets.

The setup for this example includes the VLAN **VLAN200** on the switch.

[Figure 28 on page 424](#) illustrates the topology for this example.

Figure 28: Network Topology for Using CoS Forwarding Classes to Prioritize Snooped and Inspected Packets



The components of the topology for this example are shown in [Table 26 on page 425](#).

Table 26: Components of the Topology for Using CoS Forwarding Classes to Prioritize Snooped and Inspected Packets

Properties	Settings
Switch hardware	EX Series switch
VLAN name	VLAN200
Interfaces in VLAN200	ge-0/0/1,ge-0/0/2,ge-0/0/3,ge-0/0/8
Interface for DHCP server	ge-0/0/8

In the configuration tasks for this example, you create a user-defined forwarding class **c1**, you enable DHCP snooping and DAI on VLAN200, and you assign the snooped and inspected packets to forwarding class **c1** and queue **6**. Queues 6 and 7 are reserved for high priority, control packets. The packets that are subjected to DHCP snooping and DAI are control (not data) packets; therefore, it is appropriate to place these snooped and inspected high-priority control packets in queue 6. (Queue 7 is higher priority than queue 6 and can also be used for this purpose.)

Configuration

To configure DHCP snooping and DAI on VLAN200, and to prioritize the snooped and inspected packets:

CLI Quick Configuration

To quickly configure DHCP snooping and DAI with prioritized forwarding of snooped and inspected packets, copy the following commands and paste them into the switch terminal window:

```
[edit]
set class-of-service forwarding-classes class c1 queue 6
set ethernet-switching-options security-access-port vlan VLAN200 examine-dhcp forwarding-class c1
set ethernet-switching-options security-access-port vlan VLAN200 arp-inspection forwarding-class c1
```

Step-by-Step Procedure

Configure DHCP and DAI with prioritized forwarding of snooped and inspected packets:

- Create a user-defined forwarding class to be used for prioritizing the snooped and inspected packets.

```
[edit class-of-service]
user@switch# set forwarding-classes class c1 queue 6
```
- Enable DHCP snooping on the VLAN and apply forwarding class **c1** to the snooped packets:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan VLAN200 examine-dhcp forwarding-class c1
```
- Enable DAI on the VLAN and apply forwarding class **c1** to the inspected packets:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan VLAN200 arp-inspection forwarding-class c1
```

Results

Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
vlan VLAN200 {
  arp-inspection forwarding-class c1;
  examine-dhcp forwarding-class c1;
}
[edit class-of-service]
user@switch# show
}
forwarding-classes {
  class c1 queue-num 6;
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying That Prioritized Forwarding Is Working Correctly on the Snooped Packets on page 426](#)
- [Verifying That Prioritized Forwarding Is Working Correctly on the DAI Inspected Packets on page 427](#)

[Verifying That Prioritized Forwarding Is Working Correctly on the Snooped Packets](#)

Purpose Verify that prioritized forwarding is working on the DHCP snooped packets.

Action Send some DHCP requests from network devices to the switch. Display the output queue for one of the interfaces in VLAN200 to make sure that the packets are being transmitted in the designated queue:

```
user@switch> show interfaces ge 0/0/1 extensive
```

```
Egress queues: 8 supported, 5 in use
```

Queue counters:	Queued packets	Transmitted packets	Dropped packets
0 best-effort	0	0	0
1 assured-forw	0	0	0
5 expedited-fo	0	0	0
6 c1	0	3209	0
7 network-cont	0	126371	0

Meaning The command output shows that packets have been transmitted on forwarding class c1 queue 6.

Continue testing by changing the setting of **examine-dhcp forwarding-class** to use one of the default queues, such as best-effort, and repeat the **show interfaces** command to compare the difference in the output. You can tell that the setting is working correctly by seeing the difference in the number of transmitted packets reported for forwarding class **c1** queue 6.

Verifying That Prioritized Forwarding Is Working Correctly on the DAI Inspected Packets

Purpose Verify that prioritized forwarding is working on the DAI inspected packets.

Action Send some ARP requests from network devices to the switch. Display the output queue for one of the interfaces in VLAN200 to make sure that the packets are being transmitted in the designated queue:

```
user@switch> show interfaces ge-0/0/1 extensive
```

```
Egress queues: 8 supported, 5 in use
```

Queue counters:	Queued packets	Transmitted packets	Dropped packets
0 best-effort	0	0	0
1 assured-forw	0	0	0
5 expedited-fo	0	0	0
6 c1	0	3209	0
7 network-cont	0	126371	0

Meaning The command output shows that packets have been transmitted on forwarding class **c1** queue 6.

Continue testing by changing the setting of **arp-inspection forwarding-class** to use one of the default queues, such as best-effort, and repeat the **show interfaces** command to compare the difference in the output. You can tell that the setting is working correctly by seeing the difference in the number of transmitted packets reported for forwarding class **c1** queue 6.

Related Documentation

- [Example: Protecting Against ARP Spoofing Attacks on page 418](#)

CHAPTER 16

DHCP Option 82

- [Understanding DHCP Option 82 on page 429](#)
- [Example: Setting Up DHCP Option 82 on page 433](#)
- [Example: Setting Up DHCP Option 82 \(No Relay\) on page 438](#)

Understanding DHCP Option 82

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect supported Juniper devices against attacks including spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation.

In a common scenario, various hosts are connected to the network via untrusted access interfaces on the switch, and these hosts request and are assigned IP addresses from the DHCP server. Bad actors can spoof DHCP requests using forged network addresses, however, to gain an improper connection to the network.

To protect against this vulnerability, RFC 3046, *DHCP Relay Agent Information Option*, <http://tools.ietf.org/html/rfc3046> describes a standard known as Option 82 which defines how for the DHCP server can use the location of a DHCP client when assigning IP addresses or other parameters to the client.

- [DHCP Option 82 Overview on page 429](#)
- [Suboption Components of Option 82 on page 430](#)
- [Switching Device Configurations That Support Option 82 on page 431](#)
- [DHCPv6 Options on page 432](#)

DHCP Option 82 Overview

If DHCP option 82 is enabled on a VLAN or bridge domain, then when a network device—a DHCP client—that is connected to the VLAN or bridge domain on an untrusted interface sends a DHCP request, the switching device inserts information about the client's network location into the packet header of that request. The switching device then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or another parameter for the client. See [“Suboption Components of Option 82” on page 430](#) for more information about option 82.



NOTE: On EX4300 switches, DHCP option 82 information is added to DHCP packets received on trusted interfaces as well as untrusted interfaces.

If option 82 is enabled on a VLAN or bridge domain, the following sequence of events occurs when a DHCP client sends a DHCP request:

1. The switching device receives the request and inserts the option 82 information in the packet header.
2. The switching device forwards (or relays) the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response to the switching device. It does not alter the option 82 information.
4. The switching device strips the option 82 information from the response packet.
5. The switching device forwards the response packet to the client.

To use the DHCP option 82 feature, you must ensure that the DHCP server is configured to accept option 82. If the DHCP server is not configured to accept option 82, then when it receives requests containing option 82 information, it does not use the information for setting parameters and it does not echo the information in its response message.



NOTE: If your switching device is an EX Series switch and uses Junos OS with Enhanced Layer 2 Software (ELS) configuration style, you can enable DHCP option 82 only for a specific VLAN. See [“Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\)” on page 439](#).

If your switching device is an EX Series switch and does *not* use Junos OS with Enhanced Layer 2 Software (ELS) configuration style, you can enable DHCP option 82 either for a specific VLAN or for all VLANs. See [“Setting Up DHCP Option 82 on the Switch with No Relay \(non-ELS\)” on page 441](#).

Suboption Components of Option 82

Option 82 as implemented on a switching device comprises the suboptions circuit ID, remote ID, and vendor ID. These suboptions are fields in the packet header:

- circuit ID—Identifies the circuit (interface or VLAN) on the switching device on which the request was received. The circuit ID contains the interface name and VLAN name, with the two elements separated by a colon—for example, ge-0/0/10:vlan1, where ge-0/0/10 is the interface name and vlan1 is the VLAN name. If the request packet is received on a Layer 3 interface, the circuit ID is just the interface name—for example, ge-0/0/10.

Use the prefix option to add an optional prefix to the circuit ID. If you enable the prefix option, the hostname for the switching device is used as the prefix; for example, `device1:ge-0/0/10:vlan1`, where `device1` is the hostname.

You can also specify that the interface description be used rather than the interface name or that the VLAN ID be used rather than the VLAN name.

- **remote ID**—Identifies the remote host. See [remote-id](#) for details.
- **vendor ID**—Identifies the vendor of the host. If you specify the **vendor-id** option but do not enter a value, the default value Juniper is used. To specify a value, you type a character string.

Switching Device Configurations That Support Option 82

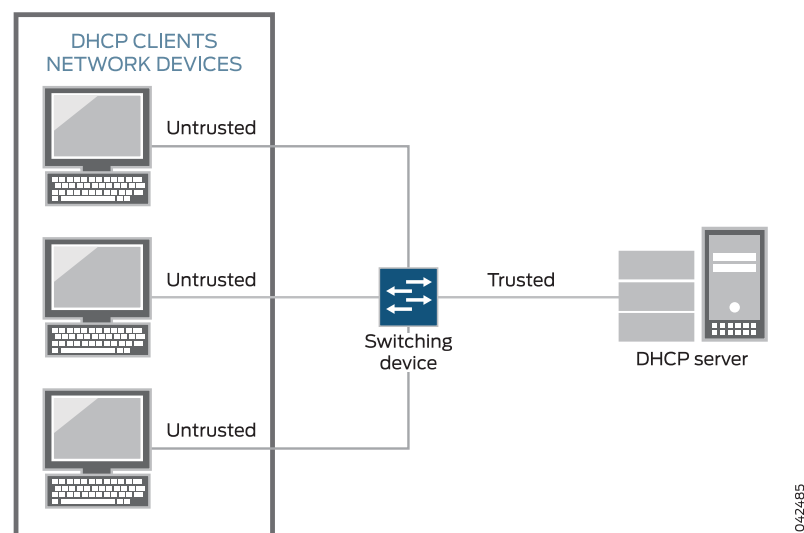
Switching device configurations that support option 82 are:

- [Switching Device, DHCP Clients, and the DHCP Server Are on the Same VLAN or Bridge Domain on page 431](#)
- [Switching Device Acts as a Relay Agent on page 432](#)

Switching Device, DHCP Clients, and the DHCP Server Are on the Same VLAN or Bridge Domain

If the switching device, the DHCP clients, and the DHCP server are all on the same VLAN or bridge domain, the switching device forwards the requests from the clients on untrusted access interfaces to the server on a trusted interface. See [Figure 29 on page 431](#).

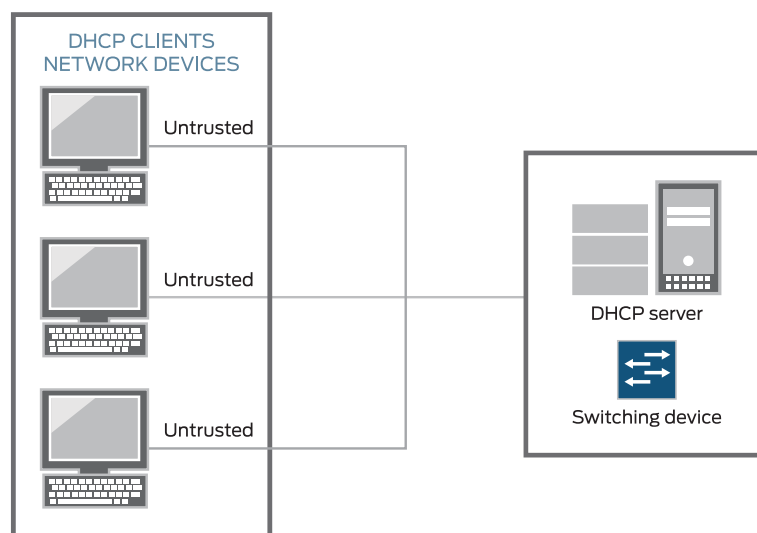
Figure 29: DHCP Clients, Switching Device, and the DHCP Server Are All on the Same VLAN or Bridge Domain



Switching Device Acts as a Relay Agent

The switching device functions as a relay agent (extended relay server) when the DHCP clients or the DHCP server is connected to the switching device through a Layer 3 interface. On the switching device, these interfaces are configured as routed VLAN interfaces (RVIs). [Figure 30 on page 432](#) illustrates a scenario for the switching device acting as an extended relay server; in this instance, the switching device relays requests to the server. This figure shows the relay agent and server on the same network, but they can also be on different networks—that is, the relay agent can be external.

Figure 30: Switching Device Acting as an Extended Relay Server



DHCPv6 Options

DHCPv6 provides several options that can be used to insert information into the DHCPv6 request packets that are relayed to a server from a client. These options are equivalent to the sub-options of DHCP option 82.

- Option 37—Identifies the remote host. Option 37 is equivalent to the **remote-id** sub-option of DHCP option 82.
- Option 18—Identifies the interface on which the DHCP request packet was received from the client. Option 18 is equivalent to the **circuit-id** sub-option of DHCP option 82.
- Option 16—Identifies the vendor of the hardware on which the client is hosted. Option 16 is equivalent to the **vendor-id** sub-option of DHCP option 82.

DHCPv6 options are not enabled automatically when DHCPv6 snooping is enabled on a VLAN. They must be configured using the [dhcpv6-options](#) statement.

Related Documentation

- [Example: Setting Up DHCP Option 82 on page 433](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\) on page 439](#)

Example: Setting Up DHCP Option 82

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.

You can configure the DHCP option 82 feature in various topologies:

- The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as routed VLAN interfaces, or RVIs. The switch relays the clients' requests to the server and then forwards the server's replies to the clients.
 - For EX Series switches, the configuration for this topology is the same for both Enhanced Layer 2 Software (ELS) and non-ELS.
- The switch, DHCP clients, and DHCP server are all on the same VLAN. The switch forwards the clients' requests to the server and forwards the server's replies to the clients.
 - If your switch is an EX Series, see [“Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\)” on page 439](#) for both ELS and non-ELS instructions.
- The switching device, DHCP clients, and DHCP server are all on the same bridge domain. The switching device forwards the clients' requests to the server and forwards the server's responses to the clients. This topic describes this configuration.

Before you configure DHCP option 82 on the switch, make sure the DHCP server is configured to accept DHCP option 82. If the server is not configured for DHCP option 82, the server does not use the DHCP option 82 information in the requests sent to it when it formulates its reply messages.

- [Example: Setting Up DHCP Option 82 on a VLAN on page 433](#)
- [Configuring DHCP Option 82 on a Router with Bridge Domain on page 437](#)

Example: Setting Up DHCP Option 82 on a VLAN

Requirements

This example describes how to configure DHCP option 82 on a switch that acts as a relay agent and is on the same VLAN as the DHCP clients, but is on a different VLAN from the DHCP server. The example includes the following hardware and software components:

- One EX4200-24P switch or one QFX3500 switch
- Junos OS Release 9.3 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Overview and Topology

In this example, you configure option 82 on the switch. The switch is configured as a BOOTP relay agent (See *DHCP/BOOTP Relay for Switches Overview* for more information). The switch connects to the DHCP server through the routed VLAN interface (RVI), as described for QFX in *Configuring IRB Interfaces on Switches* and for EX Series switches in *Configuring Routed VLAN Interfaces on Switches (CLI Procedure)*. The switch and clients are members of the **employee** VLAN (for details, see *Configuring VLANs on Switches* for the EX and QFX Series). The DHCP server is a member of the **corporate** VLAN.

If DHCP option 82 is enabled on the switch, then when a network device—a DHCP client—that is connected to the switch on an untrusted interface sends a DHCP request, the switch inserts information about the client's network location into the packet header of that request. The switch then sends the request (in this setting, it relays the request) to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or other parameter for the client.

When option 82 is enabled on the switch, then this sequence of events occurs when a DHCP client sends a DHCP request:

1. The switch receives the request and inserts the option 82 information in the packet header.
2. The switch relays the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response back to the switch. It does not alter the option 82 information.
4. The switch strips the option 82 information from the response packet.
5. The switch forwards the response packet to the client.

Configuration

To configure DHCP option 82:

CLI Quick Configuration

To quickly configure DHCP option 82, copy the following commands and paste them into the switch terminal window:

```
set forwarding-options helpers bootp dhcp-option82
set forwarding-options helpers bootp dhcp-option82 circuit-id prefix hostname
set forwarding-options helpers bootp dhcp-option82 circuit-id use-vlan-id
set forwarding-options helpers bootp dhcp-option82 remote-id
set forwarding-options helpers bootp dhcp-option82 remote-id prefix mac
set forwarding-options helpers bootp dhcp-option82 remote-id use-string employee-switch1
set forwarding-options helpers bootp dhcp-option82 vendor-id
```

Step-by-Step Procedure

To configure DHCP option 82 (replace values in *italics* with values for your own network):

1. Specify DHCP option 82 for the **employee** VLAN on the BOOTP server.

- On all interfaces that connect to the server:

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82
```

- On a specific interface that connects to the server:

```
[edit forwarding-options helpers bootp]
user@switch# set interface ge-0/0/10 dhcp-option82
```

The remaining steps are optional. They show configurations for all interfaces; include the specific interface designation to configure any of the following options on a specific interface:

2. Configure a prefix for the circuit ID suboption (the prefix is always the hostname of the switch):

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 circuit-id prefix hostname
```

3. To specify that the circuit ID suboption value should contain the interface description rather than the interface name (the default):



NOTE: When you use the interface description rather than the interface name, the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 circuit-id use-interface-description
```

4. Specify that the circuit ID suboption value contains the VLAN ID rather than the VLAN name (the default):

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 circuit-id use-vlan-id
```

5. Specify that the remote ID suboption be included in the DHCP option 82 information:

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id
```

6. Configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id prefix mac
```

- Or, to specify that the prefix for the remote ID suboption be the hostname of the switch rather than the MAC address of the switch (the default):

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id prefix hostname
```

To specify that the remote ID suboption value should contain the interface description:

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id use-interface-description
```

7. Specify that the remote ID suboption value contains a character string (here, the string is **employee-switch1**):

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 remote-id use-string employee-switch1
```

8. Configure a vendor ID suboption value, and use the default value. To use the default value, (which is **Juniper**), do not type a character string after the **vendor-id** option keyword. Otherwise, specify a value such as show here:

```
[edit forwarding-options helpers bootp]
user@switch# set dhcp-option82 vendor-id mystring
```

Results To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Check the results of the configuration:

```
[edit forwarding-options helpers bootp]
user@switch# show
dhcp-option82 {
  circuit-id {
    prefix hostname;
    use-vlan-id;
  }
  remote-id {
    prefix mac;
    use-string employee-switch1;
  }
  vendor-id;
}
```

- See Also**
- [Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443](#)
 - [Understanding DHCP Option 82 on page 429](#)
 - RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.

Configuring DHCP Option 82 on a Router with Bridge Domain

Before you configure DHCP option 82 on the switching device, perform these tasks:

- Connect and configure the DHCP server.



NOTE: Your DHCP server must be configured to accept DHCP option 82. If the server is not configured for DHCP option 82, the server does not use the DHCP option 82 information in the requests sent to it when it formulates its reply messages.

- Configure a bridge domain on the switching device and associate the interfaces on which the clients and the server connect, to the switch with that bridge domain.

To configure DHCP option 82:

1. Specify DHCP option 82 for the bridge domain that you configured:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security]
user@device# set option-82
```



NOTE: If you want to enable DHCP option 82 on all bridge domains, you must configure it separately for each specific bridge domain.

The remaining steps are optional.

2. Configure the prefix for the circuit ID suboption to include the hostname or the routing instance name for the bridge domain:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set circuit-id prefix (host-name | routing-instance-name)
```

3. Specify that the circuit ID suboption value contains the interface description rather than the interface name (the default):

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set circuit-id use-interface-description
```

4. Specify that the circuit ID suboption value contains the VLAN ID rather than the VLAN name (the default):

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set circuit-id use-vlan-id
```

5. Specify that the remote ID suboption is included in the DHCP option 82 information:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set remote-id
```



NOTE: If you do not specify a keyword after **remote-id**, the default value for the **remote-id** suboption is the interface name.

6. Specify that the remote ID suboption is the hostname of the switch:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set remote-id host-name
```

7. Specify that the remote ID suboption value contains the interface description:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set remote-id use-interface-description
```

8. Specify that the remote ID suboption value contains a character string:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set remote-id use-string mystring
```

9. Configure a vendor ID suboption:

- To use the default value (the default value is **Juniper**), do not type a character string after the **vendor-id** option keyword:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set vendor-id
```

- To configure it so that the vendor ID suboption value contains a character string value that you specify rather than **Juniper** (the default):

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82]
user@device# set vendor-id use-string mystring
```

- See Also**
- [Understanding DHCP Option 82 on page 429](#)
 - [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

Example: Setting Up DHCP Option 82 (No Relay)

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Option 82 provides information about

the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.



NOTE: DHCP option 82 is not supported on the QFX10000 switches.

You can configure the DHCP option 82 feature in several topologies:

- The switch, DHCP clients, and DHCP server are all on the same VLAN. The switch forwards the clients' requests to the server and forwards the server's replies to the clients. This topic describes this configuration.
- The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. This means that the relay agent and server can be on different networks—that is, the relay agent can be external. On the switch, these interfaces are configured as routed VLAN interfaces (RVIs) or, the interfaces are configured as integrated routing and bridging (IRB) interfaces. In either case, the switch relays the clients' requests to the server and then forwards the server's replies to the clients. These configurations are described in [“Example: Setting Up DHCP Option 82” on page 433](#).

Before you configure DHCP option 82 on the switch, perform these tasks:

- Connect and configure the DHCP server.



NOTE: Your DHCP server must be configured to accept DHCP option 82. If the server is not configured for DHCP option 82, the server does not use the DHCP option 82 information in the requests sent to it when it formulates its reply messages.

- Configure a VLAN on the switch and associate the interfaces on which the clients and the server connect to the switch with that VLAN. See *Configuring VLANs for EX Series Switches with ELS Support (CLI Procedure)*
- [Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\) on page 439](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay \(non-ELS\) on page 441](#)
- [Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443](#)

Setting Up DHCP Option 82 on the Switch with No Relay (ELS)



NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see [“Setting Up DHCP Option 82 on the Switch with No Relay \(non-ELS\)” on page 441](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

To configure DHCP option 82:

1. Specify DHCP option 82 for the VLAN that you configured.

```
[edit vlans vlan-name forwarding-options dhcp-security]  
user@switch# set option-82
```



NOTE: If you want to enable DHCP option 82 on all VLANs, you must configure it separately for each specific VLAN.

The remaining steps are optional.

2. Configure the prefix for the circuit ID suboption to include the switch's hostname or the routing instance name for the VLAN:

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]  
user@switch# set circuit-id prefix (host-name | routing-instance-name)
```

3. Specify that the circuit ID suboption value contains the interface description rather than the interface name (the default):

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]  
user@switch# set circuit-id use-interface-description
```



NOTE: Starting in Junos OS Release 14.1X53-D25, when you use the interface description rather than the interface name, the interface description has to be specified under interface unit. When you use the interface description rather than the interface name, the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.

4. Specify that the circuit ID suboption value contains the VLAN ID rather than the VLAN name (the default):

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]  
user@switch# set circuit-id use-vlan-id
```

5. Specify that the remote ID suboption is included in the DHCP option 82 information:

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]  
user@switch# set remote-id
```



NOTE: If you do not specify a keyword after *remote-id*, the default value for the *remote-id* suboption is the interface name.

6. Specify that the remote ID suboption is the hostname of the switch:

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]
user@switch# set remote-id host-name
```

7. Specify that the remote ID suboption value contains the interface description:

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]
user@switch# set remote-id use-interface-description
```

8. Specify that the remote ID suboption value contains a character string:

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]
user@switch# set remote-id use-string mystring
```

9. Configure a vendor ID suboption:

- To use the default value (the default value is **Juniper**), do not type a character string after the **vendor-id** option keyword:

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]
user@switch# set vendor-id
```

- To configure that the vendor ID suboption value contains a character string value that you specify rather than **Juniper** (the default):

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]
user@switch# set vendor-id use-string mystring
```

- See Also**
- [Example: Setting Up DHCP Option 82 on page 433](#)
 - RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.

Setting Up DHCP Option 82 on the Switch with No Relay (non-ELS)



NOTE: This task uses Junos OS for EX Series switches that do not include support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does support ELS, see “[Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\)](#)” on page 439. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

To configure DHCP option 82:



NOTE: Replace values displayed in *italics* with values for your configuration.

1. Specify DHCP option 82 for all VLANs associated with the switch or for a specified VLAN. (You can also configure the feature for a VLAN range.)

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all dhcp-option82
```

The remaining steps are optional.

2. To configure a prefix for the circuit ID suboption (the prefix is always the hostname of the switch):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 circuit-id prefix hostname
```

3. To specify that the circuit ID suboption value should contain the interface description rather than the interface name (the default):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 circuit-id use-interface-description
```



NOTE: When you use the interface description rather than the interface name, the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.

4. To specify that the circuit ID suboption value should contain the VLAN ID rather than the VLAN name (the default):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 circuit-id use-vlan-id
```

5. To specify that the remote ID suboption be included in the DHCP option 82 information:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id
```

6. To configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id prefix mac
```

7. To specify that the prefix for the remote ID suboption be the hostname of the switch rather than the MAC address of the switch (the default):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id prefix hostname
```

8. To specify that the remote ID suboption value should contain the interface description:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id use-interface-description
```

9. To specify that the remote ID suboption value should contain a character string:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id use-string mystring
```

10. To configure a vendor ID suboption and use the default value (the default value is **Juniper**), do not type a character string after the **vendor-id** option keyword:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 vendor-id
```

11. To specify that the vendor ID suboption value should contain a character string value that you specify rather than **Juniper** (the default):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 vendor-id mystring
```

To view results of the configuration steps before committing the configuration, type the **show** command at the user prompt.

To commit these changes to the active configuration, type the **commit** command at the user prompt.

See Also • RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.

Example: Setting Up DHCP Option 82 Using the Same VLAN

This example describes how to configure DHCP option 82 on a switch with DHCP clients, DHCP server, and switch all on the same VLAN:

- [Requirements on page 443](#)
- [Overview and Topology on page 444](#)
- [Configuration on page 445](#)

Requirements

This example uses the following hardware and software components:

- One EX Series or QFX Series switch

- Junos OS Release 9.3 or later for EX Series switches or Junos OS Release 12.1 or later for the QFX Series
- A DHCP server to provide IP addresses to network devices on the switch

Overview and Topology

If DHCP option 82 is enabled on the switch, then when a network device—a DHCP client—that is connected to the switch on an untrusted interface sends a DHCP request, the switch inserts information about the client's network location into the packet header of that request. The switch then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or other parameter for the client.

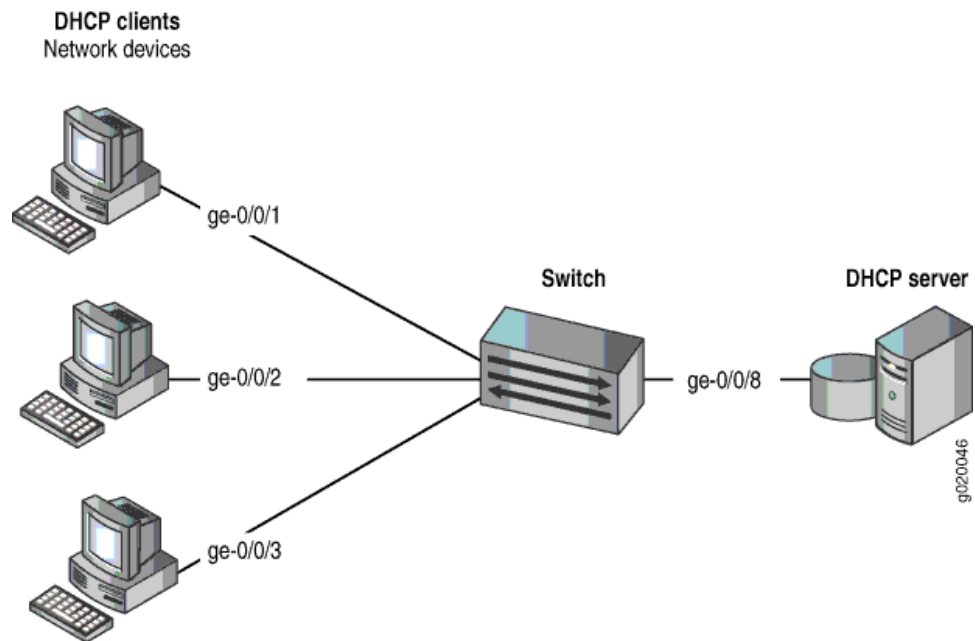
DHCP option 82 is enabled on an individual VLAN or on all VLANs on the switch.

When option 82 is enabled on the switch, then this sequence of events occurs when a DHCP client sends a DHCP request:

1. The switch receives the request and inserts the option 82 information in the packet header.
2. The switch forwards the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response back to the switch. It does not alter the option 82 information.
4. The switch strips the option 82 information from the response packet.
5. The switch forwards the response packet to the client.

[Figure 31 on page 445](#) illustrates the topology for this example.

Figure 31: Network Topology for Configuring DHCP Option 82 on a Switch That Is on the Same VLAN as the DHCP Clients and the DHCP Server



In this example, you configure DHCP option 82 on the switch. The switch connects to the DHCP server on interface `ge-0/0/8`. The DHCP clients connect to the switch on interfaces `ge-0/0/1`, `ge-0/0/2`, and `ge-0/0/3`.

The switch, server, and clients are all members of the **employee** VLAN – be sure to configure the **employee** VLAN on the switch and associated the interfaces on which the clients and the server connect to the switch with the **employee** VLAN.

Configuration

CLI Quick Configuration To quickly configure DHCP option 82, copy the following commands and paste them into the switch terminal window:

```
set ethernet-switching-options secure-access-port vlan employee dhcp-option82
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 circuit-id prefix
hostname
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 circuit-id
use-vlan-id
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 remote-id
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 remote-id
prefix mac
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 remote-id
use-string employee-switch1
set ethernet-switching-options secure-access-port vlan employee dhcp-option82 vendor-id
```

**Step-by-Step
Procedure**

To configure DHCP option 82:

1. Specify DHCP option 82 for the **employee** VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82
```

2. Configure a prefix for the circuit ID suboption (the prefix is always the hostname of the switch):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 circuit-id prefix hostname
```

3. Specify that the circuit ID suboption value contains the VLAN ID rather than the VLAN name (the default):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 circuit-id use-vlan-id
```

4. Specify that the remote ID suboption be included in the DHCP option 82 information:

```
[edit ethernet-switching-options secure-accessswitch# set vlan employee
dhcp-option82 remote-id
```

5. Configure a prefix for the remote ID suboption (here, the prefix is the MAC address of the switch):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id prefix mac
```

6. Specify that the remote ID suboption value contain a character string (here, the string is **employee-switch1**):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 remote-id use-string employee-switch1
```

7. Configure a vendor ID suboption value, and use the default value. To use the default value, do not type a character string after the **vendor-id** option keyword:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee dhcp-option82 vendor-id
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options secure-access-port]
user@switch# show
vlan employee {
  dhcp-option82 {
    circuit-id {
      prefix hostname;
      use-vlan-id;
    }
    remote-id {
```

```
    prefix mac;  
    use-string employee-switch1;  
  }  
  vendor-id;  
}  
}
```

- See Also**
- [Example: Setting Up DHCP Option 82 on page 433](#)
 - RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.
 - *Configuring VLANs for EX Series Switches*
 - *Configuring VLANs on Switches for the QFX Series*

Dynamic ARP Inspection (DAI)

- [Understanding and Using Dynamic ARP Inspection \(DAI\) on page 449](#)
- [Configuring Static ARP Table Entries For Mapping IP Addresses to MAC Addresses on page 454](#)

Understanding and Using Dynamic ARP Inspection (DAI)

Dynamic ARP inspection (DAI) protects switching devices against Address Resolution Protocol (ARP) packet spoofing (also known as ARP poisoning or ARP cache poisoning).

DAI inspects ARPs on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP spoofing. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. When an attacker tries to use a forged ARP packet to spoof an address, the switch compares the address with entries in the database. If the media access control (MAC) address or IP address in the ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped

- [Understanding ARP Spoofing and Inspection on page 449](#)
- [Enabling Dynamic ARP Inspection \(ELS\) on page 451](#)
- [Enabling Dynamic ARP Inspection \(non-ELS\) on page 452](#)
- [Applying CoS Forwarding Classes to Prioritize Inspected Packets on page 453](#)
- [Verifying That DAI Is Working Correctly on page 453](#)

Understanding ARP Spoofing and Inspection

ARP packets are sent to the Routing Engine and are rate-limited to protect the switching device from CPU overload.

- [Address Resolution Protocol on page 450](#)
- [ARP Spoofing on page 450](#)
- [Dynamic ARP Inspection on page 450](#)
- [Prioritizing Inspected Packets on page 451](#)

Address Resolution Protocol

Sending IP packets on a multi-access network requires mapping an IP address to an Ethernet MAC address.

Ethernet LANs use ARP to map MAC addresses to IP addresses.

The switching device maintains this mapping in a cache that it consults when forwarding packets to network devices. If the ARP cache does not contain an entry for the destination device, the host (the DHCP client) broadcasts an ARP request for that device's address and stores the response in the cache.

ARP Spoofing

ARP spoofing is one way to initiate man-in-the-middle attacks. The attacker sends an ARP packet that spoofs the MAC address of another device on the LAN. Instead of the switching device sending traffic to the proper network device, it sends the traffic to the device with the spoofed address that is impersonating the proper device. If the impersonating device is the attacker's machine, the attacker receives all the traffic from the switch that must have gone to another device. The result is that traffic from the switching device is misdirected and cannot reach its proper destination.

One type of ARP spoofing is gratuitous ARP, which is when a network device sends an ARP request to resolve its own IP address. In normal LAN operation, gratuitous ARP messages indicate that two devices have the same MAC address. They are also broadcast when a network interface card (NIC) in a device is changed and the device is rebooted, so that other devices on the LAN update their ARP caches. In malicious situations, an attacker can poison the ARP cache of a network device by sending an ARP response to the device that directs all packets destined for a certain IP address to go to a different MAC address instead.

To prevent MAC spoofing through gratuitous ARP and through other types of spoofing, the switches examine ARP responses through DAI.

Dynamic ARP Inspection

DAI examines ARP requests and responses on the LAN and validates ARP packets. The switch intercepts ARP packets from an access port and validates them against the DHCP snooping database. If no IP-MAC entry in the database corresponds to the information in the ARP packet, DAI drops the ARP packet and the local ARP cache is not updated with the information in that packet. DAI also drops ARP packets when the IP address in the packet is invalid. ARP probe packets are not subjected to dynamic ARP inspection. The switch always forwards such packets.

Junos OS for EX Series switches and the QFX Series uses DAI for ARP packets received on access ports because these ports are untrusted by default. Trunk ports are trusted by default, and therefore ARP packets bypass DAI on them.

You configure DAI for each VLAN, not for each interface (port). By default, DAI is disabled for all VLANs.

If you set an interface to be a DHCP trusted port, it is also trusted for ARP packets.

**NOTE:**

- If your switching device is an EX Series switch and uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, see [“Enabling a Trusted DHCP Server \(ELS\)” on page 372](#) for information about configuring an access interface to be a DHCP trusted port.

For packets directed to the switching device to which a network device is connected, ARP queries are broadcast on the VLAN. The ARP responses to those queries are subjected to the DAI check.

For DAI, all ARP packets are trapped to the Packet Forwarding Engine. To prevent CPU overloading, ARP packets destined for the Routing Engine are rate-limited.

If the DHCP server goes down and the lease time for an IP-MAC entry for a previously valid ARP packet runs out, that packet is blocked.

Prioritizing Inspected Packets



NOTE: Prioritizing inspected packets is not supported on the QFX Series and the EX4600 switch.

You can use class-of-service (CoS) forwarding classes and queues to prioritize DAI packets for a specified VLAN. This type of configuration places inspected packets for that VLAN in the egress queue, that you specify, ensuring that the security procedure does not interfere with the transmission of high-priority traffic.

Enabling Dynamic ARP Inspection (ELS)



NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see [“Enabling Dynamic ARP Inspection \(non-ELS\)” on page 452](#).



NOTE: On EX9200 switches, DHCP snooping, DAI, and IP source guard are not supported in an MC-LAG scenario.

Dynamic ARP inspection (DAI) protects switches against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP cache poisoning.

Before you can enable DAI on a VLAN, you must configure the VLAN. See *Configuring VLANs for EX Series Switches with ELS Support (CLI Procedure)*.

To enable DAI on a VLAN by using the CLI:

```
[edit vlans vlan-name forwarding-options dhcp-security]  
user@switch# set arp-inspection
```

- See Also**
- [Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487](#)

Enabling Dynamic ARP Inspection (non-ELS)



NOTE: This task uses Junos OS for EX Series switches that do not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does support ELS, see [“Enabling Dynamic ARP Inspection \(ELS\)” on page 451](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Dynamic ARP inspection (DAI) protects switches against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP cache poisoning.

- [Enabling DAI on a VLAN on page 452](#)
- [Enabling DAI on a bridge domain on page 452](#)

Enabling DAI on a VLAN

You configure DAI for each VLAN, not for each interface (port). By default, DAI is disabled for all VLANs.

To enable DAI on a VLAN or all VLANs:

- On a single VLAN:

```
[edit ethernet-switching-options secure-access-port]  
user@switch# set vlan vlan-name arp-inspection
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]  
user@switch# set vlan all arp-inspection
```

Enabling DAI on a bridge domain

See *Configuring a Bridge Domain* to set up a bridge domain if necessary.

- To enable DAI on a bridge domain:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security]  
user@device# set arp-inspection
```

- See Also**
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)

- [Example: Prioritizing Snooped and Inspected Packet on page 423](#)
- *Monitoring Port Security*

Applying CoS Forwarding Classes to Prioritize Inspected Packets

You might need to use class of service (CoS) to protect packets from critical applications from being dropped during periods of network congestion and delay and you might also need the port security features of DHCP snooping on the same ports through which those critical packets are entering and leaving.

To apply CoS forwarding classes and queues to DAI packets:

1. Create a user-defined forwarding class to be used for prioritizing DAI packets:

```
[edit class-of-service]
user@switch# set forwarding-classes class class-name queue queue-number
```

2. Enable DAI on a specific VLAN or on all VLANs and apply the desired forwarding class on the DAI packets:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan vlan-name arp-inspection forwarding-class class-name
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all arp-inspection forwarding-class class-name
```

Verifying That DAI Is Working Correctly

Purpose Verify that dynamic ARP inspection (DAI) is working on the switch.

Action Send some ARP requests from network devices connected to the switch.

Display the DAI information:

```
user@switch> show arp inspection statistics
```

ARP inspection statistics:

Interface	Packets received	ARP inspection pass	ARP inspection failed
ge-0/0/1.0	7	5	2
ge-0/0/2.0	10	10	0
ge-0/0/3.0	12	12	0

Meaning The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries

in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

- See Also**
- [Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks on page 406](#)
 - [Example: Protecting Against ARP Spoofing Attacks on page 418](#)

Configuring Static ARP Table Entries For Mapping IP Addresses to MAC Addresses

By default, the device responds to an Address Resolution Protocol (ARP) request only if the destination address of the ARP request is on the local network of the incoming interface. For Fast Ethernet or Gigabit Ethernet interfaces, you can configure static ARP entries that associate the IP addresses of nodes on the same Ethernet subnet with their media access control (MAC) addresses. These static ARP entries enable the device to respond to ARP requests even if the destination address of the ARP request is not local to the incoming Ethernet interface.

Also, unlike dynamically learned ARP entries, static ARP entries do not age out. You can also configure static ARP entries in a troubleshooting situation or if your device is unable to learn a MAC address dynamically.



NOTE: By default, an ARP policer is installed that is shared among all the Ethernet interfaces on which you have configured the `family inet` statement. By including the `arp` statement at the `[edit interfaces interface-name unit logical-unit-number family inet policer]` hierarchy level, you can apply a specific ARP-packet policer to an interface. This feature is not available on EX Series switches.

To configure static ARP entries:

1. In the configuration mode, at the `[edit]` hierarchy level, configure the router interface on which the ARP table entries for the router is configured.

```
[edit]
user@host# edit interfaces interface-name
```

2. Configure the protocol family, the logical unit of the interface, and the interface address of the router interface at the `[edit interfaces interface-name]` hierarchy level. While configuring the protocol family, specify `inet` as the protocol family.



NOTE: When you need to conserve IP addresses, you can configure an Ethernet interface to be unnumbered by including the `unnumbered-address` statement at the `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy level.

```
[edit interfaces interface-name]
user@host# edit unit logical-unit-number family inet address interface-address
```

3. Configure a static ARP entry by specifying the IP address and the MAC address that are to be mapped to each other. The IP address specified must be part of the subnet defined in the enclosing **address** statement. The MAC address must be specified as hexadecimal bytes in the following formats: *nnnn.nnnn.nnnn* or *nn:nn:nn:nn:nn:nn* format. For instance, you can use either **0011.2233.4455** or **00:11:22:33:44:55**.

```
[edit interfaces interface-name unit logical-unit-number family inet address
interface-address]
user@host# set arp ip-address mac mac-address
```

4. Configure another static ARP entry by specifying the IP address and the MAC address that are to be mapped to each other. You can also associate a multicast MAC address with a unicast IP address by including the **multicast-mac** option with the **arp** statement. You can optionally configure the router to respond to ARP requests for the specified IP address by using the **publish** option with the **arp** statement.



NOTE: For unicast MAC addresses only, if you include the **publish** option, the router or switch replies to proxy ARP requests.

```
[edit interfaces interface-name unit logical-unit-number family inet address
interface-address]
user@host# set arp ip-address multicast-mac mac-address publish
```



NOTE: The Junos OS supports the IPv6 static neighbor discovery cache entries, similar to the static ARP entries in IPv4.

Related Documentation

- *arp*
- *Management Ethernet Interface Overview*
- *Applying Policers*
- *Configuring an Unnumbered Interface*
- *Ethernet Interfaces Feature Guide for Routing Devices*

PART 7

IP Source Guard

- [Understanding IP Source Guard on page 459](#)
- [IP Source Guard Examples on page 467](#)

CHAPTER 18

Understanding IP Source Guard

- [Understanding IP Source Guard for Port Security on Switches on page 459](#)
- [Configuring IP Source Guard \(non-ELS\) on page 461](#)
- [Configuring IP Source Guard \(ELS\) on page 465](#)
- [Verifying That IP Source Guard Is Working Correctly on page 466](#)

Understanding IP Source Guard for Port Security on Switches

Ethernet LAN switches are vulnerable to attacks that involve spoofing (forging) of source IP addresses or source MAC addresses. You can use the IP source guard access port security feature to mitigate the effects of these attacks.

- [IP Address Spoofing on page 459](#)
- [How IP Source Guard Works on page 459](#)
- [IPv6 Source Guard on page 460](#)
- [The DHCP Snooping Table on page 460](#)
- [Typical Uses of Other Junos OS Features with IP Source Guard on page 461](#)

IP Address Spoofing

Hosts on access interfaces can spoof source IP addresses and source MAC addresses by flooding the switch with packets containing invalid addresses. Such attacks combined with other techniques such as TCP SYN flood attacks can cause denial-of-service (DoS) attacks. With source IP address or source MAC address spoofing, the system administrator cannot identify the source of the attack. The attacker can spoof addresses on the same subnet or on a different subnet.

How IP Source Guard Works

IP source guard examines each packet sent from a host attached to an untrusted access interface on the switch. The IP address, MAC address, VLAN and interface associated with the host is checked against entries stored in the DHCP snooping database. If the packet header does not match a valid entry in the DHCP snooping database, the switch does not forward the packet—that is, the packet is discarded.

**NOTE:**

- If your switch uses Junos OS for EX Series with support for the Enhanced Layer 2 Software (ELS) configuration style, DHCP snooping is enabled automatically when you enable IP source guard on a VLAN. See [“Configuring IP Source Guard \(ELS\)”](#) on page 465.
- If your switch uses Junos OS for EX Series without support the Enhanced Layer 2 Software (ELS) configuration style and you enable IP source guard on a VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to the VLAN. See [“Configuring IP Source Guard \(non-ELS\)”](#) on page 461.

IP source guard examines packets sent from untrusted access interfaces on those VLANs. By default, access interfaces are untrusted and trunk interfaces are trusted. IP source guard does not examine packets that have been sent to the switch by devices connected to trusted interfaces so that a DHCP server can be connected to that interface to provide dynamic IP addresses.



NOTE: On an EX9200 switch, you can set a trunk interface as **untrusted** so that it supports IP source guard.

IPv6 Source Guard

IPv6 source guard is available on switches that support DHCPv6 snooping. To determine whether your switch supports DHCPv6 snooping, see [Feature Explorer](#).

The DHCP Snooping Table

IP source guard obtains information about IP address to MAC address bindings (IP-MAC binding) from the DHCP snooping table, also known as the DHCP binding table. The DHCP snooping table is populated either through dynamic DHCP snooping or through configuration of specific static IP address to MAC address bindings. For more information about the DHCP snooping table, see [“Understanding DHCP Snooping \(ELS\)”](#) on page 385.

To display the DHCP snooping table, issue the operational mode command that appears in the switch CLI.

For DHCP snooping:

- (For non-ELS switches) [show ip-source-guard](#)
- (ELS switches only) [show dhcp-security binding](#)

For DHCPv6 snooping:

- (For non-ELS switches) [show dhcpv6 snooping binding](#)
- (ELS switches only) [show dhcp-security ipv6 binding](#)

Typical Uses of Other Junos OS Features with IP Source Guard

You can configure IP source guard with various other port security features including:

- VLAN tagging (used for voice VLANs)
- GRES (graceful Routing Engine switchover)
- Virtual Chassis configurations
- Link aggregation groups (LAGs)
- 802.1X user authentication in single supplicant, single-secure supplicant, or multiple supplicant mode.



NOTE: While implementing 801.X user authentication in single-secure supplicant or multiple supplicant mode, use the following configuration guidelines:

- If the 802.1X interface is part of an untagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has untagged membership. This also applies to IPv6 source guard and DHCPv6 snooping.
- If the 802.1X interface is part of a tagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has tagged membership. This also applies to IPv6 source guard and DHCPv6 snooping.

Related Documentation

- [Understanding DHCP Snooping \(non-ELS\) on page 393](#)
- [Configuring IP Source Guard \(ELS\) on page 465](#)
- [Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487](#)
- [Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 492](#)

Configuring IP Source Guard (non-ELS)

You can use the IP source guard access port security feature on EX Series switches to mitigate the effects of source IP address spoofing and source MAC address spoofing. If IP source guard determines that a host connected to an access interface has sent a packet with an invalid source IP address or source MAC address in the packet header, it ensures that the switch does not forward the packet—that is, the packet is discarded.

You enable the IP source guard feature on VLANs. You can enable it on a specific VLAN, on all VLANs, or on a VLAN range.



NOTE: IP source guard applies only to access interfaces and only to untrusted interfaces. If you enable IP source guard on a VLAN that includes trunk interfaces or an interface set to **dhcp-trusted**, the CLI shows an error when you try to commit the configuration.



NOTE: You can use IP source guard together with 802.1X user authentication in single supplicant, single-secure supplicant, or multiple supplicant mode.

While implementing 801.X user authentication in single-secure supplicant or multiple supplicant mode, use the following configuration guidelines:

- If the 802.1X interface is part of an untagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has untagged membership.
- If the 802.1X interface is part of a tagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has tagged membership.

- [Configuring IP Source Guard on page 462](#)
- [Configuring IPv6 Source Guard on page 463](#)
- [Disabling IP Source Guard on page 464](#)

Configuring IP Source Guard

Before you configure IP source guard, be sure that you have:

Explicitly enabled DHCP snooping on the specific VLAN or specific VLANs on which you will configure IP source guard. See [“Enabling DHCP Snooping \(non-ELS\)” on page 400](#). If you configure IP source guard on specific VLANs rather than on all VLANs, you must also enable DHCP snooping explicitly on those VLANs. Otherwise, the default value of no DHCP snooping applies to that VLAN.

To configure IP source guard:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name ip-source-guard
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all ip-source-guard
```

- On a VLAN range:

1. Set the VLAN range:

```
[edit vlans]
user@switch# set vlan-name vlan-range vlan-id-low-vlan-id-high
```

2. Associate an interface with the VLAN-range and set the port mode to **access**:

```
[edit interfaces]
user@switch# set interface-name unit 0 family ethernet-switching port-mode access vlan
members vlan-name
```

3. Enable IP source guard on the VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name ip-source-guard
```

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Configuring IPv6 Source Guard

Before you configure IPv6 source guard, be sure that you have:

- Explicitly enabled DHCPv6 snooping on the specific VLAN or specific VLANs on which you will configure IPv6 source guard. See [“Enabling DHCP Snooping \(non-ELS\)” on page 400](#). If you configure IPv6 source guard on specific VLANs rather than on all VLANs, you must also enable DHCPv6 snooping explicitly on those VLANs. Otherwise, the default value of no DHCPv6 snooping applies to that VLAN.
- Set the maximum number of IPv6 source guard sessions:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set ipv6-source-guard-sessions max-number maximum-number
```



NOTE: After setting or changing the maximum number of IPv6 source guard sessions and committing the configuration, you must reboot the switch for the configuration to take effect.

To configure IPv6 source guard:

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name ipv6-source-guard
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all ipv6-source-guard
```

- On a VLAN range:

1. Set the VLAN range):

```
[edit vlans]
user@switch# set vlan-name vlan-range vlan-id-low-vlan-id-high
```

2. Associate an interface with a VLAN-range and set the port mode to **access**:

```
[edit interfaces]
user@switch# set interface-name unit 0 family ethernet-switching port-mode access vlan
members vlan-name
```

3. Enable IPv6 source guard on the VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name ipv6-source-guard
```

To commit these changes to the active configuration, type the **commit** command at the user prompt.

Disabling IP Source Guard

You can disable IP source guard for a specific VLAN after you have enabled the feature for all VLANs, or for all VLANs.

- To disable IP source guard on a specific VLAN:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name no-ip-source-guard
```

- To disable IP source guard on all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all no-ipv6-source-guard
```



NOTE: Replace `no-ip-source-guard` with `no-ipv6-source-guard` to disable IPv6 source guard.

Related Documentation

- [Verifying That IP Source Guard Is Working Correctly on page 466](#)
- [Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 467](#)
- [Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 476](#)
- [Understanding IP Source Guard for Port Security on Switches on page 459](#)

Configuring IP Source Guard (ELS)



NOTE: This task uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switching device runs software that does not support ELS, see [“Configuring IP Source Guard \(non-ELS\)”](#) on [page 461](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.



NOTE: On EX9200 switches, IP source guard is not supported in an MC-LAG scenario.

You can use the IP source guard access port security feature to mitigate the effects of source IP address spoofing and source MAC address spoofing. If IP source guard determines that a host connected to an access interface has sent a packet with an invalid source IP address or source MAC address in the packet header, then IP source guard ensures that the switch does not forward the packet—that is, the packet is discarded.

You configure the IP source guard feature on a specific VLAN. When you configure IP source guard on a VLAN, the switch automatically enables DHCP snooping on that VLAN.

IPv6 source guard is supported on switches with support for DHCPv6 snooping. On these switches, configuring IP source guard or IPv6 source guard on a VLAN automatically enables DHCP snooping and DHCPv6 snooping on that VLAN.

IP source guard and IPv6 source guard can be applied only to untrusted interfaces. Access interfaces are untrusted by default.

IP source guard and IPv6 source guard can be used together with 802.1X user authentication in single supplicant, single-secure supplicant, or multiple supplicant mode.

Before you can configure IP source guard or IPv6 source guard on a VLAN, you must configure the VLAN. See the documentation that describes setting up basic bridging and a VLAN for your switch.

To configure IP source guard on a specific VLAN by using the CLI:

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set ip-source-guard
```

To configure IPv6 source guard on a specific VLAN by using the CLI:

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set ipv6-source-guard
```

Related Documentation

- [Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487](#)
- [Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 492](#)

- [Understanding IP Source Guard for Port Security on Switches](#) on page 459

Verifying That IP Source Guard Is Working Correctly

Purpose Verify that IP source guard is enabled and is mitigating the effects of any source IP spoofing attacks on the EX Series switch.

Action Display the IP source guard database.

```
user@switch> show ip-source-guard
```

IP source guard information:

Interface	Tag	IP Address	MAC Address	VLAN
ge-0/0/12.0	0	10.10.10.7	00:30:48:92:A5:9D	vlan100
ge-0/0/13.0	0	10.10.10.9	00:30:48:8D:01:3D	vlan100
ge-0/0/13.0	100	*	*	voice

Meaning The IP source guard database table contains the VLANs enabled for IP source guard, the untrusted access interfaces on those VLANs, the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another. If a switch interface is associated with multiple VLANs and some of those VLANs are enabled for IP source guard and others are not, the VLANs that are not enabled for IP source guard have a star (*) in the **IP Address** and **MAC Address** fields. See the entry for the **voice** VLAN in the preceding sample output.

Related Documentation • [Configuring IP Source Guard \(non-ELS\)](#) on page 461

CHAPTER 19

IP Source Guard Examples

- [Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 467](#)
- [Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 476](#)
- [Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487](#)
- [Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 492](#)
- [Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing on page 497](#)
- [Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 497](#)
- [Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 502](#)

Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN

Ethernet LAN switches are vulnerable to attacks that involve spoofing (forging) of source IP addresses or source MAC addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. You can enable the IP source guard port security feature on EX Series switches to mitigate the effects of such attacks. If IP source guard determines that a source IP address and a source MAC address in a binding in an incoming packet are not valid, the switch does not forward the packet.

If two VLANs share an interface, you can configure IP source guard on just one of the VLANs; in this example, you configure IP source guard on an untagged data VLAN but not on the tagged voice VLAN. You can use 802.1X user authentication to validate the device connections on the data VLAN.

This example describes how to configure IP source guard with 802.1X user authentication on a data VLAN, with a voice VLAN on the same interface:

- [Requirements on page 468](#)
- [Overview and Topology on page 468](#)

- [Configuration on page 469](#)
- [Verification on page 472](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 9.2 or later for EX Series switches
- A DHCP server to provide IP addresses to network devices on the switch
- A RADIUS server to provide 802.1X authentication

Before you configure IP source guard for the data VLANs, be sure you have:

- Connected the DHCP server to the switch.
- Connected the RADIUS server to the switch and configured user authentication on the server. See *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*.
- Configured the VLANs. See *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches* for detailed information about configuring VLANs.

Overview and Topology

IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the switch. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the switch does not forward the packet—that is, the packet is discarded.

When you configure IP source guard, you enable it on one or more VLANs. IP source guard applies its checking rules to untrusted access interfaces on those VLANs. By default, on EX Series switches, access interfaces are untrusted and trunk interfaces are trusted. IP source guard does not check packets that have been sent to the switch by devices connected to either trunk interfaces or trusted access interfaces—that is, interfaces configured with **dhcp-trusted** so that a DHCP server can be connected to that interface to provide dynamic IP addresses.

IP source guard obtains information about IP-address/MAC-address/VLAN bindings from the DHCP snooping database. It causes the switch to validate incoming IP packets against the entries in that database.

The topology for this example includes one EX-3200-24P switch, a PC and an IP phone connected on the same interface, a connection to a DHCP server, and a connection to a RADIUS server for user authentication.



NOTE: The 802.1X user authentication applied in this example is for single supplicants.

You can also use IP source guard with 802.1X user authentication for single-secure supplicant or multiple supplicant mode. If you are implementing IP source guard with 802.1X authentication in single-secure supplicant or multiple supplicant mode, you must use the following configuration guidelines:

- If the 802.1X interface is part of an untagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has untagged membership.
- If the 802.1X interface is part of a tagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has tagged membership.



TIP: You can set the `ip-source-guard` flag in the `traceoptions (Access Port Security)` statement for debugging purposes.

This example shows how to configure a static IP address to be added to the DHCP snooping database.

Configuration

CLI Quick Configuration To quickly configure IP source guard on a data VLAN, copy the following commands and paste them into the switch terminal window:

```
set ethernet-switching-options voip interface ge-0/0/14.0 vlan voice
set ethernet-switching-options secure-access-port interface ge-0/0/24.0 dhcp-trusted
set ethernet-switching-options secure-access-port interface ge-0/0/14 static-ip 10.1.1.1 mac
00:11:11:11:11:11 vlan data
set ethernet-switching-options secure-access-port vlan data examine-dhcp
set ethernet-switching-options secure-access-port vlan data ip-source-guard
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members data
set vlans voice vlan-id 100
set protocols lldp-med interface ge-0/0/14.0
set protocols dot1x authenticator authentication-profile-name profile52
set protocols dot1x authenticator interface ge-0/0/14.0 supplicant single
```

Step-by-Step Procedure To configure IP source guard on the data VLAN:

1. Configure the VoIP interface:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/14.0 vlan voice
```

2. Configure the interface on which the DHCP server is connected to the switch as a trusted interface and add that interface to the data VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/24.0 dhcp-trusted
[edit interfaces]
user@switch# set ge-0/0/24 unit 0 family ethernet-switching vlan members data
```

3. Configure a static IP address on an interface on the data VLAN (optional)

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/14 static-ip 10.1.1.1 mac 00:11:11:11:11
vlan data
```

4. Configure DHCP snooping and IP source guard on the data VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port vlan data examine-dhcp
user@switch# set secure-access-port vlan data ip-source-guard
```

5. Configure 802.1X user authentication and LLDP-MED on the interface that is shared by the data VLAN and the voice VLAN:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/14.0
user@switch# set dot1x authenticator authentication-profile-name profile52
user@switch# set dot1x authenticator interface ge-0/0/14.0 supplicant single
```

6. Set the VLAN ID for the voice VLAN:

```
[edit vlans]
user@switch# set voice vlan-id 100
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options]
user@switch# show
voip {
  interface ge-0/0/14.0 {
    vlan voice;
  }
}
secure-access-port {
  interface ge-0/0/14.0 {
    static-ip 10.1.1.1 vlan data mac 00:11:11:11:11;
  }
  interface ge-0/0/24.0 {
    dhcp-trusted;
  }
}
vlan data {
  examine-dhcp;
  ip-source-guard;
}
}
```

```
[edit interfaces]
ge-0/0/24 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members data;
      }
    }
  }
}
}
```

```
[edit vlans]
voice {
  vlan-id 100;
}
}
```

```
[edit protocols]
lldp-med {
  interface ge-0/0/14.0;
}
dot1x {
  authenticator {
    authentication-profile-name profile52;
  }
  interface {
    ge-0/0/14.0 {
      supplicant single;
    }
  }
}
}
```



TIP: If you wanted to configure IP source guard on the voice VLAN as well as on the data VLAN, you would configure DHCP snooping and IP source guard exactly as you did for the data VLAN. The configuration result for the voice VLAN under `secure-access-port` would look like this:

```
secure-access-port {  
  vlan voice {  
    examine-dhcp;  
    ip-source-guard;  
  }  
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying That 802.1X User Authentication Is Working on the Interface on page 472](#)
- [Verifying the VLAN Association with the Interface on page 473](#)
- [Verifying That DHCP Snooping and IP Source Guard Are Working on the Data VLAN on page 474](#)

Verifying That 802.1X User Authentication Is Working on the Interface

Purpose Verify the 802.1X configuration on interface `ge-0/0/14`.

Action Verify the 802.1X configuration with the operational mode command **show dot1x interface**:

```
user@switch> show dot1x interface ge-0/0/14.0 detail

ge-0/0/14.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: <not configured>
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning The **Supplicant mode** output field displays the configured administrative mode for each interface. Interface **ge-0/0/14.0** displays **Single** supplicant mode.

Verifying the VLAN Association with the Interface

Purpose Display the interface state and VLAN membership.

Action user@switch> show ethernet-switching interfaces

```
Ethernet-switching table: 0 entries, 0 learned
```

```
user@switch> show ethernet-switching interfaces
Interface  State  VLAN members  Blocking
ge-0/0/0.0  down  default        unblocked
ge-0/0/1.0  down  employee        unblocked
ge-0/0/2.0  down  employee        unblocked
ge-0/0/12.0 down  default        unblocked
ge-0/0/13.0 down  default        unblocked
ge-0/0/13.0 down  vlan100        unblocked
ge-0/0/14.0 up    voice          unblocked
              data          unblocked
ge-0/0/17.0 down  employee        unblocked
ge-0/0/23.0 down  default        unblocked
ge-0/0/24.0 down  data          unblocked
              employee        unblocked
              vlan100        unblocked
              voice          unblocked
```

Meaning The field **VLAN members** shows that the **ge-0/0/14.0** interface supports both the **data** VLAN and the **voice** VLAN. The **State** field shows that the interface is up.

Verifying That DHCP Snooping and IP Source Guard Are Working on the Data VLAN

Purpose Verify that DHCP snooping and IP source guard are enabled and working on the data VLAN.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp snooping binding
```

```
DHCP Snooping Information:
MAC address      IP address  Lease (seconds)  Type      VLAN      Interface
00:05:85:3A:82:77 192.0.2.17  600              dynamic   employee   ge-0/0/1.0
00:05:85:3A:82:79 192.0.2.18  653              dynamic   employee   ge-0/0/1.0
00:05:85:3A:82:80 192.0.2.19  720              dynamic   employee   ge-0/0/2.0
00:05:85:3A:82:81 192.0.2.20  932              dynamic   employee   ge-0/0/2.0
                                00:30:48:92:A5:9D 10.10.10.7 720              dynamic
vlan100 ge-0/0/13.0
00:30:48:8D:01:3D 10.10.10.9 720              dynamic   data       ge-0/0/14.0
00:30:48:8D:01:5D 10.10.10.8 1230             dynamic   voice      ge-0/0/14.0
00:11:11:11:11:11 10.1.1.1    -                static    data       ge-0/0/14.0
00:05:85:27:32:88 192.0.2.22  -                static    employee   ge-0/0/17.0
00:05:85:27:32:89 192.0.2.23  -                static    employee   ge-0/0/17.0
00:05:85:27:32:90 192.0.2.27  -                static    employee   ge-0/0/17.0
```

View the IP source guard information for the data VLAN.

```
user@switch> show ip-source-guard
```

```
IP source guard information:
Interface  Tag  IP Address  MAC Address  VLAN
ge-0/0/13.0 0    10.10.10.7  00:30:48:92:A5:9D  vlan100
ge-0/0/14.0 0    10.10.10.9  00:30:48:8D:01:3D  data
ge-0/0/14.0 0    10.1.1.1    00:11:11:11:11:11  data
ge-0/0/13.0 100  *          *             voice
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see the preceding sample output for **show dhcp snooping binding**) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires. Static IP addresses have no assigned lease time. Statically configured entries never expire.

The IP source guard database table contains the VLANs enabled for IP source guard, the untrusted access interfaces on those VLANs, the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another. If a switch interface is associated with multiple VLANs and some of those VLANs are enabled for IP source guard and others are not, the VLANs that are not enabled for IP source guard

have a star (*) in the **IP Address** and **MAC Address** fields. See the entry for the **voice** VLAN in the preceding sample output.

- Related Documentation**
- [Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 476](#)
 - [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
 - [Configuring IP Source Guard \(non-ELS\) on page 461](#)

Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces

Ethernet LAN switches are vulnerable to attacks that involve spoofing (forging) of source IP addresses or source MAC addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. You can enable the IP source guard port security feature on EX Series switches to mitigate the effects of such attacks. If IP source guard determines that a source IP address and a source MAC address in a binding in an incoming packet are not valid, the switch does not forward the packet.

You can use IP source guard in combination with other EX Series switch features to mitigate address-spoofing attacks on untrusted access interfaces. This example shows two configuration scenarios:

- [Requirements on page 476](#)
- [Overview and Topology on page 477](#)
- [Configuring IP Source Guard with 802.1X Authentication, DHCP Snooping, and Dynamic ARP Inspection on page 478](#)
- [Configuring IP Source Guard on a Guest VLAN on page 481](#)
- [Verification on page 484](#)

Requirements

This example uses the following hardware and software components:

- An EX Series switch
- Junos OS Release 9.2 or later for EX Series switches
- A DHCP server to provide IP addresses to network devices on the switch
- A RADIUS server to provide 802.1X authentication

Before you configure IP source guard for the scenarios related in this example, be sure you have:

- Connected the DHCP server to the switch.

- Connected the RADIUS server to the switch and configured user authentication on the RADIUS server. See *Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*.
- Configured VLANs on the switch. In this example, we have two VLANs, which are named **DATA** and **GUEST**. The **DATA** VLAN is configured with **vlan-id 300**. The **GUEST** VLAN (which functions as the guest VLAN) is configured with **vlan-id 100**. See *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches* for detailed information about configuring VLANs.

Overview and Topology

IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the switch. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the switch does not forward the packet—that is, the packet is discarded.

When you configure IP source guard, you enable it on one or more VLANs. IP source guard applies its checking rules to untrusted access interfaces on those VLANs. By default, on EX Series switches, access interfaces are untrusted and trunk interfaces are trusted. IP source guard does not check packets that have been sent to the switch by devices connected to either trunk interfaces or trusted access interfaces—that is, interfaces configured with **dhcp-trusted**. A DHCP server can be connected to a **dhcp-trusted** interface to provide dynamic IP addresses.

IP source guard obtains information about IP-addresses, MAC-addresses, or VLAN bindings from the DHCP snooping database, which enables the switch to validate incoming IP packets against the entries in that database.

The topology for this example includes an EX Series switch, which is connected to both a DHCP server and to a RADIUS server.



NOTE: The 802.1X user authentication applied in this example is for single-suppliant mode.

You can use IP source guard with 802.1X user authentication for single-secure supplicant or multiple supplicant mode. If you are implementing IP source guard with 802.1X authentication in single-secure supplicant or multiple supplicant mode, you must use the following configuration guidelines:

- If the 802.1X interface is part of an untagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has untagged membership.
- If the 802.1X interface is part of a tagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has tagged membership.

In the first configuration example, two clients (network devices) are connected to an access switch. You configure IP source guard and 802.1X user authentication, in combination with two access port security features: DHCP snooping and dynamic ARP inspection (DAI). This setup is designed to protect the switch from IP attacks such as *ping of death* attacks, DHCP starvation, and ARP spoofing.

In the second configuration example, the switch is configured for 802.1X user authentication. If the client fails authentication, the switch redirects the client to a guest VLAN that allows this client to access a set of restricted network features. You configure IP source guard on the guest VLAN to mitigate effects of source IP spoofing.



TIP: You can set the `ip-source-guard` flag in the `traceoptions` statement for debugging purposes.

Configuring IP Source Guard with 802.1X Authentication, DHCP Snooping, and Dynamic ARP Inspection

CLI Quick Configuration To quickly configure IP source guard with 802.1X authentication and with other access port security features, copy the following commands and paste them into the switch terminal window:

```
[edit]
set ethernet-switching-options secure-access-port interface ge-0/0/24 dhcp-trusted
set ethernet-switching-options secure-access-port vlan DATA examine-dhcp
set ethernet-switching-options secure-access-port vlan DATA arp-inspection
set ethernet-switching-options secure-access-port vlan DATA ip-source-guard
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members DATA
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members DATA
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members DATA
set protocols lldp-med interface ge-0/0/0.0
set protocols dot1x authenticator authentication-profile-name profile52
set protocols dot1x authenticator interface ge-0/0/0.0 supplicant single
set protocols lldp-med interface ge-0/0/1.0
set protocols dot1x authenticator interface ge-0/0/1.0 supplicant single
```

Step-by-Step Procedure To configure IP source guard with 802.1X authentication and various port security features:

1. Configure the interface on which the DHCP server is connected to the switch as a trusted interface and add that interface to the **DATA** VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/24 dhcp-trusted
user@switch# set set ge-0/0/24 unit 0 family ethernet-switching vlan members DATA
```

2. Associate two other access interfaces (untrusted) with the DATA VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching vlan members DATA
user@switch# set ge-0/0/1 unit 0 family ethernet-switching vlan members DATA
```

3. Configure 802.1X user authentication and LLDP-MED on the two interfaces that you associated with the DATA VLAN:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/0.0
user@switch# set dot1x authenticator authentication-profile-name profile52
user@switch# set dot1x authenticator interface ge-0/0/0.0 supplicant single
user@switch# set lldp-med interface ge-0/0/1.0
user@switch# set dot1x authenticator interface ge-0/0/1.0 supplicant single
```

4. Configure three access port security features—DHCP snooping, dynamic ARP inspection (DAI), and IP source guard—on the **DATA** VLAN:

```
[edit ethernet-switching-options]
user@switch# set secure-access-port vlan DATA examine-dhcp
user@switch# set secure-access-port vlan DATA arp-inspection
user@switch# set secure-access-port vlan DATA ip-source-guard
```

Results Check the results of the configuration:

```
[edit ethernet-switching-options]
secure-access-port {
  interface ge-0/0/24.0 {
    dhcp-trusted;
  }
  vlan DATA {
    arp-inspection;
    examine-dhcp;
    ip-source-guard;
  }
}
```

```
[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members DATA;
      }
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members DATA;
      }
    }
  }
}
ge-0/0/24 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members DATA;
      }
    }
  }
}
```

```
[edit protocols]
lldp-med {
  interface ge-0/0/0.0;
  interface ge-0/0/1.0;
}
dot1x {
  authenticator {
    authentication-profile-name profile52;
  }
}
```

```

interface {
  ge-0/0/0.0 {
    suppliant single;
  }
  ge-0/0/1.0 {
    suppliant single;
  }
}

```

Configuring IP Source Guard on a Guest VLAN

CLI Quick Configuration To quickly configure IP source guard on a guest VLAN, copy the following commands and paste them into the switch terminal window:

```

[edit]
set ethernet-switching-options secure-access-port interface ge-0/0/24 dhcp-trusted
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members GUEST
set ethernet-switching-options secure-access-port vlan GUEST examine-dhcp
set ethernet-switching-options secure-access-port vlan GUEST ip-source-guard
set ethernet-switching-options secure-access-port interface ge-0/0/0 static-ip 10.1.1.1 mac
00:11:11:11:11:11 vlan GUEST
set ethernet-switching-options secure-access-port interface ge-0/0/1 static-ip 10.1.1.2 mac
00:22:22:22:22:22 vlan GUEST
set interfaces ge-0/0/0 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/1 unit 0 family ethernet-switching port-mode access
set protocols dot1x authenticator authentication-profile-name profile52
set protocols dot1x authenticator interface ge-0/0/0 suppliant single
set protocols dot1x authenticator interface ge-0/0/0 guest-vlan GUEST
set protocols dot1x authenticator interface ge-0/0/0 suppliant-timeout 2
set protocols dot1x authenticator interface ge-0/0/1 suppliant single
set protocols dot1x authenticator interface ge-0/0/1 guest-vlan GUEST
set protocols dot1x authenticator interface ge-0/0/1 suppliant-timeout 2

```

Step-by-Step Procedure To configure IP source guard on a guest VLAN:

1. Configure the interface on which the DHCP server is connected to the switch as a trusted interface and add that interface to the **GUEST** VLAN:

```

[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/24 dhcp-trusted
user@switch# set ge-0/0/24 unit 0 family ethernet-switching vlan members GUEST

```

2. Configure two interfaces for the access port mode:

```

[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching port-mode access
user@switch# set ge-0/0/1 unit 0 family ethernet-switching port-mode access

```

3. Configure DHCP snooping and IP source guard on the **GUEST** VLAN:

```

[edit ethernet-switching-options]
user@switch# set secure-access-port vlan GUEST examine-dhcp
user@switch# set secure-access-port vlan GUEST ip-source-guard

```

4. Configure a static IP address on each of two (untrusted) interfaces on the **GUEST** VLAN (optional):

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/0 static-ip 10.1.1.1 mac 00:11:11:11:11
vlan GUEST
```

```
[edit ethernet-switching-options]
user@switch# set secure-access-port interface ge-0/0/1 static-ip 10.1.1.2 mac
00:22:22:22:22:22 vlan GUEST
```

5. Configure 802.1X user authentication:

```
[edit protocols]
user@switch# set dot1x authenticator authentication-profile-name profile52
user@switch# set dot1x authenticator interface ge-0/0/0 supplicant single
user@switch# set dot1x authenticator interface ge-0/0/1 supplicant single
user@switch# set dot1x authenticator interface ge-0/0/0 supplicant-timeout 2
user@switch# set dot1x authenticator interface ge-0/0/1 supplicant-timeout 2
```

Results Check the results of the configuration:

```
[edit protocols]
dot1x {
  authenticator {
    authentication-profile-name profile52;
  }
  interface {
    ge-0/0/0.0 {
      guest-vlan GUEST;
      supplicant single;
      supplicant-timeout 2;
    }
    ge-0/0/1.0 {
      guest-vlan GUEST;
      supplicant single;
      supplicant-timeout 2;
    }
  }
}
}
```

```
[edit vlans]
GUEST {
  vlan-id 100;
}
```

```
[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
    }
  }
}
ge-0/0/24 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members GUEST;
      }
    }
  }
}
```

```
[edit ethernet-switching-options]
secure-access-port {
  interface ge-0/0/0.0 {
    static-ip 10.1.1.1 vlan GUEST mac 00:11:11:11:11;
  }
  interface ge-0/0/1.0 {
    static-ip 10.1.1.2 vlan GUEST mac 00:22:22:22:22:22;
  }
  interface ge-0/0/24.0 {
    dhcp-trusted;
  }
  vlan GUEST {
    examine-dhcp;
    ip-source-guard;
  }
}
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying That 802.1X User Authentication Is Working on the Interface on page 484](#)
- [Verifying the VLAN Association with the Interface on page 485](#)
- [Verifying That DHCP Snooping Is Working on the VLAN on page 486](#)
- [Verifying That IP Source Guard Is Working on the VLAN on page 486](#)

Verifying That 802.1X User Authentication Is Working on the Interface

Purpose Verify that the 802.1X configuration is working on the interface.

Action user@switch> show dot1x interface ge/0/0/0.0 detail

```

ge-0/0/0.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 2
  Quiet period: 30 seconds
  Transmit period: 15 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 2 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 1
  Guest VLAN member: GUEST
  Number of connected supplicants: 1
    Supplicant: md5user01, 00:30:48:90:53:B7
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Radius
      Authenticated VLAN: DATA
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3581 seconds

```

Meaning The **Supplicant mode** field displays the configured administrative mode for each interface. The **Guest VLAN member** field displays the VLAN to which a supplicant is connected when the supplicant is authenticated using a guest VLAN. The **Authenticated VLAN** field displays the VLAN to which the supplicant is connected.

Verifying the VLAN Association with the Interface

Purpose Verify interface states and VLAN memberships.

Action user@switch> show ethernet-switching interfaces

Interface	State	VLAN members	Tag	Tagging	Blocking
ge-0/0/0.0	up	DATA	101	untagged	unblocked
ge-0/0/1.0	up	DATA	101	untagged	unblocked
ge-0/0/24	up	DATA	101	untagged	unblocked

Meaning The **VLAN members** field shows the associations between VLANs and interfaces. The **State** field shows whether the interfaces are up or down.

For the guest VLAN configuration, the interface is associated with the guest VLAN if and when the supplicant fails 802.1X user authentication.

Verifying That DHCP Snooping Is Working on the VLAN

Purpose Verify that DHCP snooping is enabled and working on the VLAN. Send some DHCP requests from network devices (DHCP clients) connected to the switch.

Action user@switch> [show dhcp snooping binding](#)

```
DHCP Snooping Information:
MAC address      IP address      Lease (seconds) Type    VLAN    Interface
00:30:48:90:53:B7 192.0.2.1      86392    dynamic DATA    ge-0/0/24.0
```

Meaning When the interface on which the DHCP server connects to the switch has been set to **dhcp-trusted**, the output shows for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires. Static IP addresses have no assigned lease time. Statically configured entries never expire.

Verifying That IP Source Guard Is Working on the VLAN

Purpose Verify that IP source guard is enabled and working on the VLAN.

Action user@switch> [show ip-source-guard](#)

```
IP source guard information:
Interface  Tag  IP Address      MAC Address      VLAN
ge-0/0/0.0  0    192.0.2.2      00:30:48:90:63:B7 DATA
ge-0/0/1.0  0    192.0.2.3      00:30:48:90:73:B7 DATA
```

Meaning The IP source guard database table contains the VLANs for which IP source guard is enabled, the untrusted access interfaces on those VLANs, the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another. If a switch interface is associated with multiple VLANs and some of those VLANs have IP source guard enabled (or configured) while others do not have IP source guard enabled, the VLANs that do not have IP source guard enabled have a star (*) in the **IP Address** and **MAC Address** fields.

- Related Documentation**
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch](#)
 - [Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 467](#)
 - [Configuring IP Source Guard \(non-ELS\) on page 461](#)

Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing



NOTE: This example uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see [“Example: Protecting Against ARP Spoofing Attacks” on page 418](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.



NOTE: On EX9200 switches, DHCP snooping, DAI, and IP source guard are not supported in an MC-LAG scenario.

This example describes how to enable IP source guard and Dynamic ARP Inspection (DAI) on a specified VLAN to protect the switch against spoofed IP/MAC addresses and ARP spoofing attacks. When you enable either IP source guard or DAI, the configuration automatically enables DHCP snooping for the same VLAN.

- [Requirements on page 487](#)
- [Overview and Topology on page 487](#)
- [Configuration on page 489](#)
- [Verification on page 490](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100, QFX5110, and QFX5200 switches.

- One EX4300 switch or EX9200 switch
- Junos OS Release 13.2X50-D10 or later for EX Series switches
- A DHCP server to provide IP addresses to network devices on the switch

Before you configure IP source guard to prevent IP/MAC spoofing or DAI to mitigate ARP spoofing attacks, be sure you have:

- Connected the DHCP server to the switch.
- Configured the VLAN to which you are adding DHCP security features.

Overview and Topology

Ethernet LAN switches are vulnerable to attacks on security that involve spoofing (forging) of source MAC addresses or source IP addresses. These spoofed packets are sent from

hosts connected to untrusted access interfaces on the switch. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the switch against entries stored in the DHCP snooping database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the switch does not forward the packet—that is, the packet is discarded.

Another type of security attack is ARP spoofing (also known as ARP poisoning or ARP cache poisoning). ARP-spoofing is a way to initiate man-in-the-middle attacks. The attacker sends an ARP packet that spoofs the MAC address of another device on the LAN. Instead of the switch sending traffic to the proper network device, it sends it to the device with the spoofed address that is impersonating the proper device. If the impersonating device is the attacker's machine, the attacker receives all the traffic from the switch that should have gone to another device. The result is that traffic from the switch is misdirected and cannot reach its proper destination.



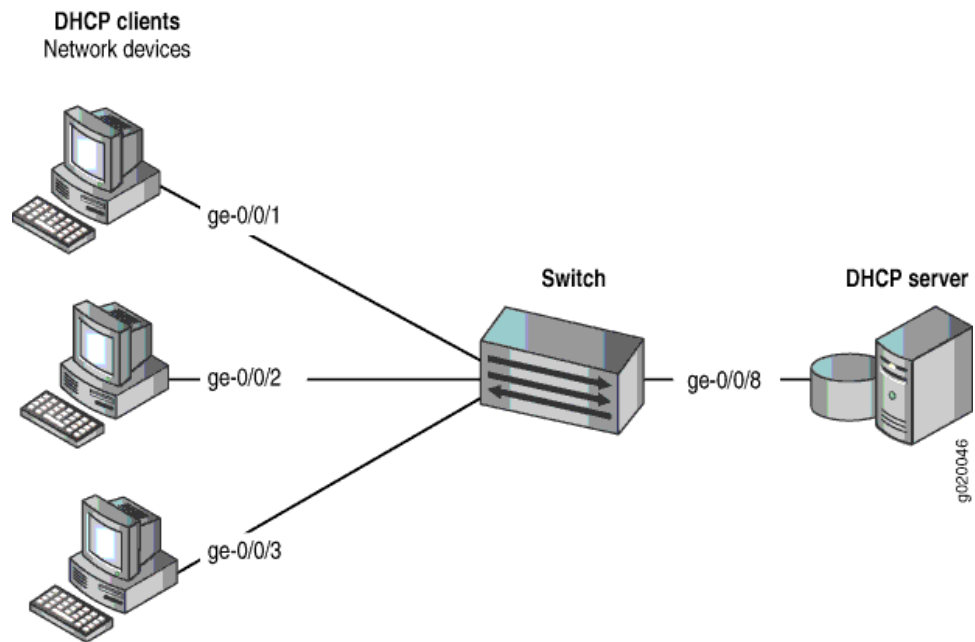
NOTE: When dynamic ARP inspection (DAI) is enabled, the switch logs the number of invalid ARP packets that it receives on each interface, along with the sender's IP and MAC addresses. You can use these log messages to discover ARP spoofing on the network.

This example shows how to configure these important port security features on a switch that is connected to a DHCP server. The setup for this example includes the VLAN **employee-vlan** on the switch. [Figure 27 on page 420](#) illustrates the topology for this example.



NOTE: The trunk interface connecting to the DHCP server interface is a trusted port by default. If you attach a DHCP server to an access port, you must configure the port as trusted. Before you do so, ensure that the server is physically secure—that is, that access to the server is monitored and controlled. For more information on trusted and untrusted ports for DHCP, see [“Understanding and Using Trusted DHCP Servers” on page 371](#).

Figure 32: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 25 on page 420](#).

Table 27: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX4300 or EX9200 switch
VLAN name and ID	employee-vlan , tag 20
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is the subnet's broadcast address
Interfaces in employee-vlan	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface connecting to DHCP server	ge-0/0/8

In this example, the switch has already been configured as follows:

- All access ports are untrusted, which is the default setting.
- The trunk port (**ge-0/0/8**) is trusted, which is the default setting.
- The VLAN (**employee-vlan**) has been configured to include the specified interfaces.

Configuration

To configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping) to protect the switch against IP spoofing and ARP attacks:

CLI Quick Configuration To quickly configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping), copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans employee-vlan forwarding-options dhcp-security ip-source-guard
set vlans employee-vlan forwarding-options dhcp-security arp-inspection
```

Step-by-Step Procedure Configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping) on the VLAN:

1. Configure IP source guard on the VLAN:

```
[edit vlans employee-vlan forwarding-options dhcp-security]
user@switch# set ip-source-guard
```

2. Enable DAI on the VLAN:

```
[edit vlans employee-vlan forwarding-options dhcp-security]
user@switch# set arp-inspection
```

Results Check the results of the configuration:

```
user@switch> show vlans employee-vlan forwarding-options
employee-vlan {
  forwarding-options {
    dhcp-security {
      arp-inspection;
      ip-source-guard;
    }
  }
}
```

Verification

Confirm that the configuration is working properly.

- [Verifying That DHCP Snooping Is Working Correctly on the Switch on page 490](#)
- [Verifying That IP Source Guard is Working on the VLAN on page 491](#)
- [Verifying That DAI Is Working Correctly on the Switch on page 491](#)

Verifying That DHCP Snooping Is Working Correctly on the Switch

Purpose Verify that DHCP snooping is working on the switch.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the port on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

user@switch> [show dhcp-security binding](#)

IP Address	MAC Address	Vlan	Expires	State	Interface
192.0.2.17	00:05:85:3A:82:77	employee-vlan	86265	BOUND	ge-0/0/1.0
192.0.2.18	00:05:85:3A:82:79	employee-vlan	86265	BOUND	ge-0/0/1.0
192.0.2.19	00:05:85:3A:82:80	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.20	00:05:85:3A:82:81	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.21	00:05:85:3A:82:83	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.22	00:05:85:27:32:88	employee-vlan	86254	BOUND	ge-0/0/3.0

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for the assigned IP address, the device's MAC address, the VLAN name, and the time, in seconds, remaining before the lease expires.

[Verifying That IP Source Guard is Working on the VLAN](#)

Purpose Verify that IP source guard is enabled and working on the VLAN.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch. View the IP source guard information for the data VLAN.

user@switch> [show dhcp-security binding ip-source-guard](#)

IP Address	MAC Address	Vlan	Expires	State	Interface
192.0.2.17	00:05:85:3A:82:77	employee-vlan	86265	BOUND	ge-0/0/1.0
192.0.2.18	00:05:85:3A:82:79	employee-vlan	86265	BOUND	ge-0/0/1.0
192.0.2.19	00:05:85:3A:82:80	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.20	00:05:85:3A:82:81	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.21	00:05:85:3A:82:83	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.22	00:05:85:27:32:88	employee-vlan	86254	BOUND	ge-0/0/3.0

Meaning The IP source guard database table contains the VLANs enabled for IP source guard.

[Verifying That DAI Is Working Correctly on the Switch](#)

Purpose Verify that DAI is working on the switch.

Action Send some ARP requests from network devices connected to the switch.

Display the DAI information:

```
user@switch> show dhcp-security arp inspection statistics
```

ARP inspection statistics:

Interface	Packets received	ARP inspection pass	ARP inspection failed
ge-0/0/1.0	7	5	2
ge-0/0/2.0	10	10	0
ge-0/0/3.0	12	12	0

Meaning The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

- Related Documentation**
- [Configuring IP Source Guard \(ELS\) on page 465](#)
 - [Enabling Dynamic ARP Inspection \(ELS\) on page 451](#)
 - [Enabling Dynamic ARP Inspection \(J-Web Procedure\)](#)

Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing



NOTE: This example uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see [“Example: Protecting Against ARP Spoofing Attacks” on page 418](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

This example describes how to enable IPv6 source guard and neighbor discovery inspection on a specified VLAN to protect the switch against IPv6 address spoofing attacks. When you enable either IPv6 source guard or neighbor discovery inspection, DHCPv6 snooping is automatically enabled on the same VLAN.

- [Requirements on page 493](#)
- [Overview and Topology on page 493](#)
- [Configuration on page 494](#)
- [Verification on page 495](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX5100, QFX5110, and QFX5200 switches.

- One EX Series switch that supports the Enhanced Layer 2 Software configuration style.
- Junos OS Release 13.2X51-D20 or later for EX Series switches
- A DHCPv6 server to provide IPv6 addresses to network devices on the switch

Before you configure IPv6 source guard and neighbor discovery inspection to prevent IPv6 address spoofing attacks, be sure you have:

- Connected the DHCPv6 server to the switch.
- Configured the VLAN to which you are adding DHCPv6 security features. See the documentation that describes setting up basic bridging and a VLAN for your switch.

Overview and Topology

Ethernet LAN switches are vulnerable to attacks on security that involve spoofing (forging) of source MAC addresses or source IPv6 addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. For more information on IPv6 address spoofing attacks, see [“IPv6 Neighbor Discovery Inspection” on page 509](#).

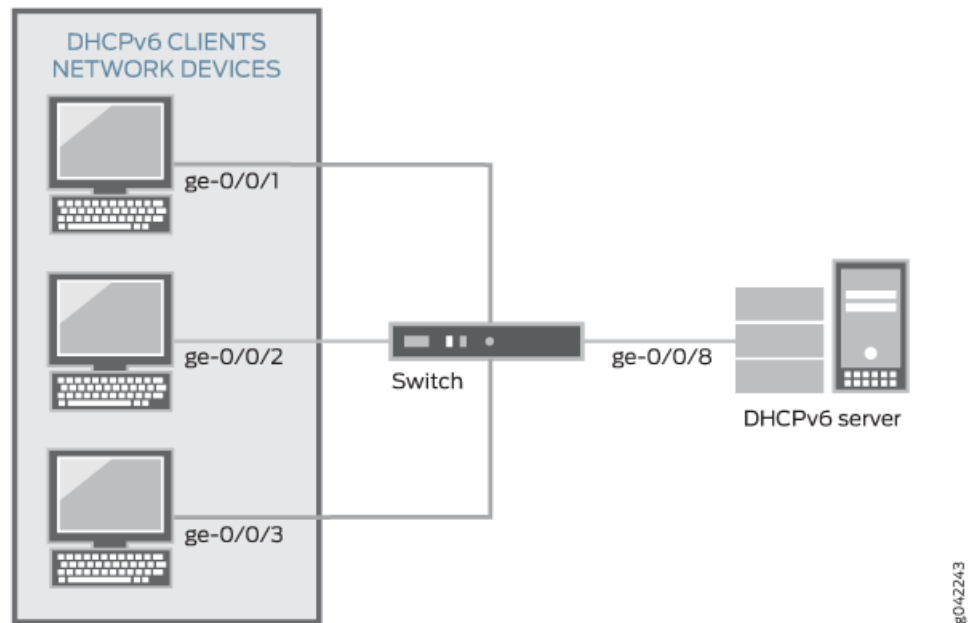
By using the DHCPv6 snooping table, also known as the binding table, IPv6 source guard and neighbor discovery inspection mitigate the risk of IPv6 spoofing attacks. The DHCPv6 snooping table contains the IP address, MAC address, VLAN and interface ID for each host associated with the VLAN. When a packet is sent from a host attached to an untrusted access interface on the switch, IPv6 source guard checks it against the entries in the DHCPv6 snooping table. If there is no match in the table, the switch does not forward the packet—that is, the packet is discarded. Neighbor discovery inspection verifies neighbor discovery messages sent between IPv6 nodes on the same network link against the DHCPv6 snooping table, and also discards the packet if no match is found.

This example shows how to configure these important port security features on a switch that is connected to a DHCPv6 server. The setup for this example includes the VLAN sales on the switch. [Figure 27 on page 420](#) illustrates the topology for this example.



NOTE: The trunk interface connecting to the DHCPv6 server interface is a trusted port by default.

Figure 33: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 25 on page 420](#).

Table 28: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX Series switch that supports the Enhanced Layer 2 Software configuration style.
VLAN name and ID	sales, tag 20
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is the subnet's broadcast address
Interfaces in sales	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface connecting to DHCPv6 server	ge-0/0/8

In this example, the switch has already been configured as follows:

- All access ports are untrusted, which is the default setting.
- The trunk port (ge-0/0/8) is trusted, which is the default setting.
- The VLAN (sales) has been configured to include the specified interfaces.

Configuration

- [\[xref target has no title\]](#)

CLI Quick Configuration To quickly configure IPv6 source guard and neighbor discovery inspection (and thereby, also automatically configure DHCPv6 snooping), copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans sales forwarding-options dhcp-security ipv6-source-guard
set vlans sales forwarding-options dhcp-security neighbor-discovery-inspection
```

Step-by-Step Procedure Configure IPv6 source guard and neighbor discovery inspection (and thereby, also automatically configure DHCPv6 snooping) on the VLAN:

1. Configure IPv6 source guard on the VLAN:

```
[edit vlans sales forwarding-options dhcp-security]
user@switch# set ipv6-source-guard
```

2. Enable neighbor discovery inspection on the VLAN:

```
[edit vlans sales forwarding-options dhcp-security]
user@switch# set neighbor-discovery-inspection
```

Results Check the results of the configuration:

```
user@switch> show vlans sales forwarding-options
dhcp-security {
  neighbor-discovery-inspection;
  ipv6-source-guard;
}
```

Verification

Confirm that the configuration is working properly.

- [Verifying That DHCPv6 Snooping Is Working Correctly on the Switch on page 495](#)
- [Verifying That Neighbor Discovery Inspection Is Working Correctly on the Switch on page 496](#)

Verifying That DHCPv6 Snooping Is Working Correctly on the Switch

Purpose Verify that DHCPv6 snooping is working on the switch.

Action Send DHCPv6 requests from network devices (in this example, these are DHCPv6 clients) connected to the switch.

Display the DHCPv6 snooping information when the port on which the DHCPv6 server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IPv6 addresses and leases:

user@switch> [show dhcp-security ipv6 binding](#)

IPv6 address	MAC address	Vlan	Expires	State	Interface
2001:db8:fe10::	00:10:94:00:55:0b	vlan20	3456	BOUND	ge-0/0/1.0
fe80::210:94ff:fe00:1	00:10:94:00:55:0b	vlan20	3456	BOUND	ge-0/0/1.0
2001:db8:fe12::	00:10:94:00:00:34	vlan20	3456	BOUND	ge-0/0/2.0
fe80::210:94ff:fe00:2	00:10:94:00:00:34	vlan20	3456	BOUND	ge-0/0/2.0
2001:db8:fe14::	00:10:94:00:00:55	vlan20	3456	BOUND	ge-0/0/3.0
fe80::210:94ff:fe00:3	00:10:94:00:00:55	vlan20	3456	BOUND	ge-0/0/3.0

Meaning The output shows the assigned IPv6 addresses, the MAC address, the VLAN name, and the time, in seconds, remaining before the lease expires. Because IPv6 hosts usually have more than one IPv6 address assigned to each of their IPv6-enabled network interfaces, there are two entries added for each client: one with the link-local IPv6 address, which is used by the client for DHCP transactions, and another with the IPv6 address assigned by the server. The link-local address always has the prefix **fe80::/10**.

[Verifying That Neighbor Discovery Inspection Is Working Correctly on the Switch](#)

Purpose Verify that neighbor discovery inspection is working on the switch.

Action Send neighbor discovery packets from network devices connected to the switch.

Display the neighbor discovery information:

user@switch> [show dhcp-security neighbor-discovery-inspection statistics](#)

ND inspection statistics:			
Interface	ND Packets received	ND inspection pass	ND inspection failed
ge-0/0/1.0	7	5	2
ge-0/0/2.0	10	10	0
ge-0/0/3.0	12	12	0

Meaning The sample output shows the number of neighbor discovery packets received and inspected per interface, with a list of the number of packets that passed and the number of packets that failed the inspection on each interface. The switch compares the neighbor discovery requests and replies against the entries in the DHCPv6 snooping database. If

a MAC address or IPv6 address in the neighbor discovery packet does not match a valid entry in the database, the packet is dropped.

- Related Documentation**
- [Configuring IP Source Guard \(ELS\) on page 465](#)
 - [Configuring Port Security \(ELS\) on page 9](#)

Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing

You can use the IP source guard access port security feature on MX Series routers to mitigate the effects of source IP address spoofing and source MAC address spoofing. If IP source guard determines that a host connected to an access interface has sent a packet with an invalid source IP address or source MAC address in the packet header, then IP source guard ensures that the switching device does not forward the packet—that is, the packet is discarded.

To configure IP source guard on a specific bridge domain by using the CLI:

- Configure the IP source guard on a bridge domain:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security]
user@device# set ip-source-guard (MX Series)
```

To configure IP source guard at the routing instance level by using the CLI:

- Configure the IP source guard at the routing instance level:

```
[edit routing-instances ri-name bridge-domains bridge-domain-name
forwarding-options dhcp-security]
user@device# set ip-source-guard (MX Series)
```

- Related Documentation**
- [ip-source-guard \(MX Series\) on page 825](#)

Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks

This example describes how to enable IP source guard and Dynamic ARP inspection (DAI) on a specified bridge domain to protect the device against spoofed IP/MAC addresses and ARP spoofing attacks. When you enable either IP source guard or DAI, the configuration automatically enables DHCP snooping for the same bridge domain.

- [Requirements on page 498](#)
- [Overview and Topology on page 498](#)
- [Configuration on page 500](#)
- [Verification on page 500](#)

Requirements

This example uses the following hardware and software components:

- One MX Series router
- Junos OS Release 14.1
- A DHCP server to provide IP addresses to network devices on the device

Before you configure IP source guard to prevent IP/MAC spoofing or DAI to mitigate ARP spoofing attacks, be sure you have:

- Connected the DHCP server to the device.
- Configured the bridge domain to which you are adding DHCP security features. See *Configuring the Bridge Domain for MX Series Router Cloud CPE Services*.

Overview and Topology

Ethernet LAN devices are vulnerable to attacks on security that involve spoofing (forging) of source MAC addresses or source IP addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the device. IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the device against entries stored in the DHCP snooping database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the device does not forward the packet—that is, the packet is discarded.

Another type of security attack is ARP spoofing (also known as ARP poisoning or ARP cache poisoning). ARP spoofing is a way to initiate man-in-the-middle attacks. The attacker sends an ARP packet that spoofs the MAC address of another device on the bridge domain. Instead of the device sending traffic to the proper network device, it sends it to the device with the spoofed address that is impersonating the proper device. If the impersonating device is the attacker's machine, the attacker receives all the traffic from the device that should have gone to another device. The result is that traffic from the device is misdirected and cannot reach its proper destination.



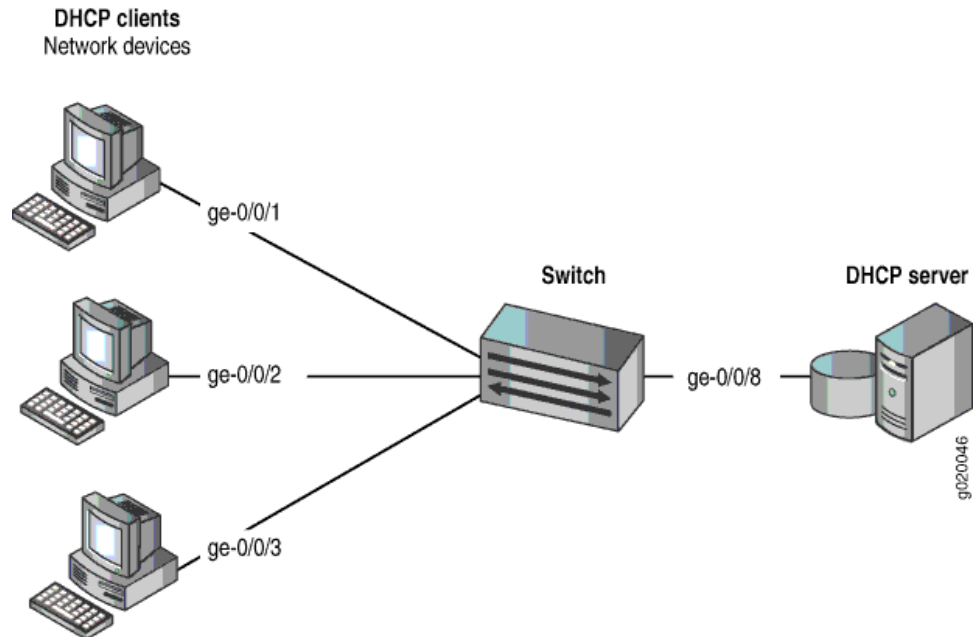
NOTE: When DAI is enabled, the device logs the number of invalid ARP packets that it receives on each interface, along with the sender's IP and MAC addresses. You can use these log messages to discover ARP spoofing on the network.

This example shows how to configure these important port security features on a device that is connected to a DHCP server. The setup for this example includes the bridge domain **employee-bdomain** on the switching device. [Figure 27 on page 420](#) illustrates the topology for this example.



NOTE: The trunk interface connecting to the DHCP server interface is a trusted port by default.

Figure 34: Switching Device Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 25 on page 420](#).

Table 29: Components of the Port Security Topology

Properties	Settings
Device hardware	One MX Series router
Bridge domain name and ID	employee-bdomain , tag 20
Bridge domain subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is the subnet's broadcast address
Interfaces in employee-bdomain	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface connecting to DHCP server	ge-0/0/8

In this example, the device has already been configured as follows:

- All access ports are untrusted, which is the default setting.
- The trunk port (ge-0/0/8) is trusted, which is the default setting.
- The bridge-domain (**employee-bdomain**) has been configured to include the specified interfaces.

Configuration

CLI Quick Configuration To quickly configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping to protect the device against IP spoofing and ARP attacks), copy the following commands and paste them into the device terminal window:

```
[edit]
set bridge-domains employee-bdomain forwarding-options dhcp-security ip-source-guard
set bridge-domains employee-bdomain forwarding-options dhcp-security arp-inspection
```

Step-by-Step Procedure To configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping) on the bridge domain:

1. Configure IP source guard on the bridge domain:

```
[edit bridge-domains employee-bdomain forwarding-options dhcp-security]
user@device# set ip-source-guard
```

2. Enable DAI on the bridge domain:

```
[edit bridge-domains employee-bdomain forwarding-options dhcp-security]
user@device# set arp-inspection
```

Results Check the results of the configuration:

```
user@device> show bridge-domains employee-bdomain forwarding-options
employee-bdomain {
  forwarding-options {
    dhcp-security {
      arp-inspection;
      ip-source-guard;
    }
  }
}
```

Verification

Confirm that the configuration is working properly.

- [Verifying That DHCP Snooping Is Working Correctly on the Device on page 500](#)
- [Verifying That IP Source Guard Is Working on the Bridge Domain on page 501](#)
- [Verifying That DAI Is Working Correctly on the Device on page 501](#)

Verifying That DHCP Snooping Is Working Correctly on the Device

Purpose Verify that DHCP snooping is working on the device.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the device.

Display the DHCP snooping information when the port on which the DHCP server connects to the device is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

user@device> [show dhcp-security binding](#)

IP Address	MAC Address	Vlan	Expires	State	Interface
192.0.2.17	00:05:85:3A:82:77	employee-vlan	86265	BOUND	ge-0/0/1.0
192.0.2.18	00:05:85:3A:82:79	employee-vlan	86265	BOUND	ge-0/0/1.0
192.0.2.19	00:05:85:3A:82:80	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.20	00:05:85:3A:82:81	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.21	00:05:85:3A:82:83	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.22	00:05:85:27:32:88	employee-vlan	86254	BOUND	ge-0/0/3.0

Meaning When the interface on which the DHCP server connects to the device has been set to trusted, the output (see the preceding sample) shows, for the assigned IP address, the device's MAC address, the VLAN name, and the time, in seconds, remaining before the lease expires.

[Verifying That IP Source Guard Is Working on the Bridge Domain](#)

Purpose Verify that IP source guard is enabled and working on the bridge domain.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the device. View the IP source guard information for the data bridge domain.

user@device> [show dhcp-security binding ip-source-guard](#)

IP Address	MAC Address	Vlan	Expires	State	Interface
192.0.2.17	00:05:85:3A:82:77	employee-vlan	86265	BOUND	ge-0/0/1.0
192.0.2.18	00:05:85:3A:82:79	employee-vlan	86265	BOUND	ge-0/0/1.0
192.0.2.19	00:05:85:3A:82:80	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.20	00:05:85:3A:82:81	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.21	00:05:85:3A:82:83	employee-vlan	86287	BOUND	ge-0/0/2.0
192.0.2.22	00:05:85:27:32:88	employee-vlan	86254	BOUND	ge-0/0/3.0

Meaning The IP source guard database table contains the VLANs and bridge domains enabled for IP source guard.

[Verifying That DAI Is Working Correctly on the Device](#)

Purpose Verify that DAI is working on the device.

Action Send some ARP requests from network devices connected to the device.

Display the DAI information:

```
user@device> show dhcp-security arp inspection statistics
```

ARP inspection statistics:

Interface	Packets received	ARP inspection pass	ARP inspection failed
ge-0/0/1.0	7	5	2
ge-0/0/2.0	10	10	0
ge-0/0/3.0	12	12	0

Meaning The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The device compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

- Related Documentation**
- [Configuring IP Source Guard \(ELS\) on page 465](#)
 - [Enabling Dynamic ARP Inspection \(ELS\) on page 451](#)

Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing

This example describes how to enable IPv6 source guard and neighbor discovery inspection on a specified VLAN to protect an EX Series switch against IPv6 address spoofing attacks. IPv6 source guard and neighbor discovery inspection support introduced on EX2200 and EX3300 switches in Junos OS Release 14.1X53-D10.

- [Requirements on page 502](#)
- [Overview and Topology on page 503](#)
- [Configuration on page 504](#)
- [Verification on page 505](#)

Requirements

This example uses the following hardware and software components:

- One EX2200 or EX3300 switch
- Junos OS Release 14.1X53-D10 or later for EX Series switches
- A DHCPv6 server to provide IPv6 addresses to network devices on the switch

Before you configure IPv6 source guard and neighbor discovery inspection to prevent IPv6 address spoofing attacks, be sure you have:

- Connected the DHCPv6 server to the switch.

- Configured the VLAN to which you are adding DHCPv6 security features. See *Configuring VLANs for EX Series Switches*.

Overview and Topology

Ethernet LAN switches are vulnerable to attacks on security that involve spoofing (forging) of source MAC addresses or source IPv6 addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. For more information on IPv6 address spoofing attacks, see [“IPv6 Neighbor Discovery Inspection” on page 509](#).

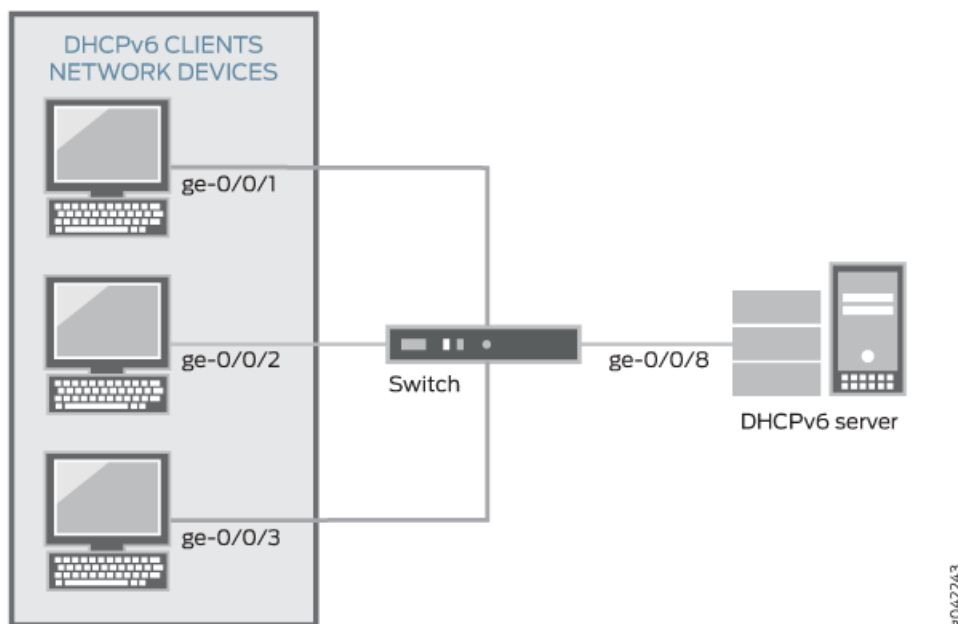
IPv6 source guard and neighbor discovery inspection mitigate the risk of IPv6 spoofing attacks by using the DHCPv6 snooping table. Also known as the binding table, the DHCPv6 snooping table contains the valid bindings of IPv6 addresses to MAC addresses. When a packet is sent from a host attached to an untrusted access interface on the switch, IPv6 source guard verifies the source IPv6 address and MAC address of the packet against the DHCPv6 snooping table. If there is no match in the table, the switch does not forward the packet—that is, the packet is discarded. Neighbor discovery inspection verifies neighbor discovery messages sent between IPv6 nodes on the same network link against the DHCPv6 snooping table, and also discards the packet if no match is found.

This example shows how to configure these important port security features on a switch that is connected to a DHCPv6 server. The setup for this example includes the VLAN **sales** on the switch. [Figure 27 on page 420](#) illustrates the topology for this example.



NOTE: The trunk interface connecting to the DHCPv6 server interface is a trusted port by default.

Figure 35: Network Topology for Basic Port Security



The components of the topology for this example are shown in [Table 25 on page 420](#).

Table 30: Components of the Port Security Topology

Properties	Settings
Switch hardware	One EX2200 or EX3300 switch
VLAN name and ID	sales, tag
VLAN subnets	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is the subnet's broadcast address
Interfaces in sales	ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8
Interface connecting to DHCPv6 server	ge-0/0/8

In this example, the switch has already been configured as follows:

- All access ports are untrusted, which is the default setting.
- The trunk port (ge-0/0/8) is trusted, which is the default setting.
- The VLAN (sales) has been configured to include the specified interfaces.

Configuration

CLI Quick Configuration To quickly configure IPv6 source guard and neighbor discovery inspection, copy the following commands and paste them into the switch terminal window:

```
[edit]
set ethernet-switching-options secure-access-port vlan sales examine-dhcpv6
set ethernet-switching-options secure-access-port vlan sales ipv6-source-guard
set ethernet-switching-options secure-access-port vlan sales neighbor-discovery-inspection
```

Step-by-Step Procedure Configure IPv6 source guard and neighbor discovery inspection (and thereby, also automatically configure DHCPv6 snooping) on the VLAN:

1. Enable DHCPv6 snooping on the VLAN:


```
[edit ethernet-switching-options secure-access-port vlan sales]
user@switch# set examine-dhcpv6
```
2. Configure IPv6 source guard on the VLAN:


```
[edit ethernet-switching-options secure-access-port vlan sales]
user@switch# set ipv6-source-guard
```
3. Configure neighbor discovery inspection on the VLAN:


```
[edit ethernet-switching-options secure-access-port vlan sales]
user@switch# set neighbor-discovery-inspection
```

Results Check the results of the configuration:

```
user@switch> show ethernet-switching-options secure-access-port
vlan sales {
  examine-dhcpv6;
  ipv6-source-guard;
  neighbor-discovery-inspection;
}
}
```

Verification

Confirm that the configuration is working properly.

- [Verifying That DHCPv6 Snooping Is Working Correctly on the Switch on page 505](#)
- [Verifying That Neighbor Discovery Inspection Is Working Correctly on the Switch on page 506](#)

Verifying That DHCPv6 Snooping Is Working Correctly on the Switch

Purpose Verify that DHCPv6 snooping is working on the switch.

Action Send DHCPv6 requests from network devices (in this example, these are DHCPv6 clients) connected to the switch.

Display the DHCPv6 snooping information when the port on which the DHCPv6 server connects to the switch is trusted. The following is the output when requests are sent from the MAC addresses and the server has provided the IPv6 addresses and leases:

```
user@switch> show dhcpv6 snooping binding
```

DHCP Snooping Information:

MAC address	IP address	Lease (seconds)	Type	VLAN	Interface
00:10:94:00:00:01	2001:db8::10:0:3	3599992	dynamic	sales	ge-0/0/1.0
00:10:94:00:00:01	fe80::210:94ff:fe00:1	3599992	dynamic	sales	ge-0/0/1.0
00:10:94:00:00:02	2001:db8::10:0:5	3599992	dynamic	sales	ge-0/0/2.0
00:10:94:00:00:02	fe80::210:94ff:fe00:2	3599992	dynamic	sales	ge-0/0/2.0
00:10:94:00:00:03	2001:db8::10:0:7	3599992	dynamic	sales	ge-0/0/3.0
00:10:94:00:00:03	fe80::210:94ff:fe00:3	3599992	dynamic	sales	ge-0/0/3.0

Meaning The output shows the assigned IP address, the MAC address, the VLAN name, and the time, in seconds, leased to the IP address. Because IPv6 hosts usually have more than one IP address assigned to each of their IPv6-enabled network interfaces, there are two entries added for each client: one with the link-local IP address, which is used by the client for DHCP transactions, and another with the IP address assigned by the server. The link-local address always has the prefix **fe80::/10**.

Verifying That Neighbor Discovery Inspection Is Working Correctly on the Switch

Purpose Verify that neighbor discovery inspection is working on the switch.

Action Send neighbor discovery packets from network devices connected to the switch.

Display the neighbor discovery information:

```
user@switch> show neighbor-discovery-inspection statistics
```

ND inspection statistics:

Interface	Packets received	ND inspection pass	ND inspection failed
ge-0/0/1.0	7	5	2
ge-0/0/2.0	10	10	0
ge-0/0/3.0	12	12	0

Meaning The sample output shows the number of neighbor discovery packets received and inspected per interface, and lists the number of packets passed and the number that failed the inspection on each interface. The switch compares the neighbor discovery requests and replies against the entries in the DHCPv6 snooping database. If a MAC address or IPv6 address in the neighbor discovery packet does not match a valid entry in the database, the packet is dropped.

Release History Table

Release	Description
14.1X53-D10	IPv6 source guard and neighbor discovery inspection support introduced on EX2200 and EX3300 switches in Junos OS Release 14.1X53-D10.

- Related Documentation**
- [Configuring IP Source Guard \(non-ELS\) on page 461](#)
 - [Enabling DHCP Snooping \(non-ELS\) on page 400](#)
 - [Configuring Port Security \(non-ELS\) on page 11](#)

PART 8

IPv6 Access Security

- [Neighbor Discovery Protocol on page 509](#)
- [Router Advertisement Guard on page 511](#)

CHAPTER 20

Neighbor Discovery Protocol

- [IPv6 Neighbor Discovery Inspection on page 509](#)

IPv6 Neighbor Discovery Inspection

- [IPv6 Neighbor Discovery Protocol Overview on page 509](#)
- [Neighbor Discovery \(ND\) Inspection on page 509](#)
- [Enabling ND Inspection on page 510](#)

IPv6 Neighbor Discovery Protocol Overview

IPv6 nodes (hosts and routers) use Neighbor Discovery Protocol (NDP) to discover the presence and link-layer addresses of other nodes residing on the same link. Hosts use NDP to find neighboring routers that are willing to forward packets on their behalf, while routers use it to advertise their presence. Nodes also use NDP to maintain reachability information about the paths to active neighbors. When a router or the path to a router fails, a host can search for alternate paths.

The NDP process is based on the exchange of neighbor solicitation and advertisement messages. NDP messages are unsecured, which makes NDP susceptible to attacks that involve the spoofing (or forging) of link-layer addresses. An attacking node can cause packets for legitimate nodes to be sent to some other link-layer address by either sending a neighbor solicitation message with a spoofed source MAC address, or by sending a neighbor advertisement address with a spoofed target MAC address. The spoofed MAC address is then associated with a legitimate network IPv6 address by the other nodes.

Neighbor Discovery (ND) Inspection

IPv6 neighbor discovery inspection mitigates NDP security vulnerabilities by inspecting neighbor discovery messages and verifying them against the DHCPv6 snooping table. The DHCPv6 snooping table, which is built by snooping DHCPv6 message exchanges, includes the IPv6 address, MAC address, VLAN and interface for each host associated with the VLAN. When a neighbor discovery message is received on an untrusted interface, neighbor discovery inspection discards the packet unless the source IPv6 and MAC addresses, VLAN, and interface can be matched to an entry in the DHCPv6 snooping table. Entries can be added to the DHCPv6 snooping table by configuring the [static-ipv6](#) CLI statement.



NOTE: Neighbor discovery messages are always allowed on trusted interfaces.

Neighbor discovery inspection verifies five different ICMPv6 message types: Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement, and Redirect. By discarding message packets that can not be verified against the DHCPv6 snooping table, neighbor discovery inspection can prevent the following types of attacks:

- Cache poisoning attacks—Neighbor discovery cache poisoning is the IPv6 equivalent of ARP spoofing, in which an attacker uses a forged address to send an unsolicited advertisement to other hosts on the network, for associating its own MAC address with a legitimate network IP address. These bindings between IPv6 addresses and MAC addresses are stored by each node in its neighbor cache. Once the caches are updated with the malicious bindings, the attacker can initiate a man-in-the-middle attack, intercepting traffic that was intended for a legitimate host.
- Routing denial-of-service (DoS) attacks—An attacker could cause a host to disable its first-hop router by spoofing the address of a router and sending a neighbor advertisement message with the *router* flag cleared. The victim host assumes that the device that used to be its first-hop router is no longer a router.
- Redirect attacks—Routers use ICMPv6 redirect requests to inform a host of a more efficient route to a destination. Hosts can be redirected to a better first-hop router, but can also be informed by a Router Redirect message that the destination is in fact a neighbor. An attacker using this provision can achieve an effect similar to cache poisoning and intercept all traffic from the victim host. Neighbor discovery inspection checks that Router Redirect messages are sent only by trusted routers.

Enabling ND Inspection



NOTE: DHCPv6 snooping is enabled automatically when neighbor discovery inspection is configured. There is no explicit configuration required for DHCPv6 snooping.

To enable neighbor discovery inspection on a VLAN:

```
[edit vlans vlan-name forwarding-options dhcp-security]  
user@switch# set neighbor-discovery-inspection
```

Related Documentation

- [Understanding DHCP Snooping \(ELS\) on page 385](#)

CHAPTER 21

Router Advertisement Guard

- [Understanding IPv6 Router Advertisement Guard on page 511](#)
- [Configuring Stateful IPv6 Router Advertisement Guard on page 514](#)
- [Configuring Stateless IPv6 Router Advertisement Guard on page 517](#)

Understanding IPv6 Router Advertisement Guard

In an IPv6 deployment, routers periodically multicast Router Advertisement (RA) messages to announce their availability and convey information to neighboring nodes that enable them to be automatically configured on the network. RA messages are used by Neighbor Discovery Protocol (NDP) to detect neighbors, advertise IPv6 prefixes, assist in address provisioning, and share link parameters such as maximum transmission unit (MTU), hop limit, advertisement intervals, and lifetime. Hosts listen for RA messages for IPv6 address autoconfiguration and discovery of link-local addresses of the neighboring routers, and can also send a Router Solicitation (RS) message to request immediate advertisements.

RA messages are unsecured, which makes them susceptible to attacks on the network that involve the spoofing (or forging) of link-layer addresses. Also, unintended misconfiguration by users or administrators might lead to the presence of unwanted, or rogue, RA messages, which can cause operational problems for neighboring hosts. You can configure IPv6 Router Advertisement (RA) guard to protect your network against rogue RA messages generated by unauthorized or improperly configured routers connecting to the network segment.

RA guard works by validating RA messages on the basis of whether they meet certain criteria, configured on the switch using policies. RA guard inspects RA messages and compares the information contained in the message attributes to the configured policy. Depending on the policy, RA guard either drops or forwards the RA messages that match the conditions.

The following information contained in RA message attributes can be used by RA guard to validate the source of the RA message:

- Source MAC address
- Source IPv6 address
- Source IPv6 address prefix

- Hop-count limit
- Router preference priority
- *Managed* configuration flag
- *Other* configuration flag

You can configure RA guard to operate in either stateless or stateful mode. In stateless mode, in the default state, an RA message that is received on an interface is examined and filtered on the basis of whether it matches the conditions configured in the policy attached to that interface. If the content of the RA message is validated, it forwards the RA message to its destination; otherwise, the RA message is dropped. The state of an interface operating in stateless mode can be changed by configuration. If the interface is configured as *trusted*, all RA messages are forwarded without being validated against the policy. If the interface is configured as *blocked*, all RA messages are dropped without being validated against the policy.

In stateful mode, an interface can dynamically transition from one state to another based on information gathered during a learning period. During this period, known as the *learning* state, ingress RA messages are validated against a policy to determine which interfaces are attached to links with valid IPv6 routers. At the end of the learning period, interfaces attached to legitimate senders of RA messages transition dynamically to the *forwarding* state, in which RA messages are forwarded if they can be validated against a policy. Interfaces that do not receive valid RA messages during the learning period transition dynamically to the *blocked* state, in which all ingress RA messages are dropped.

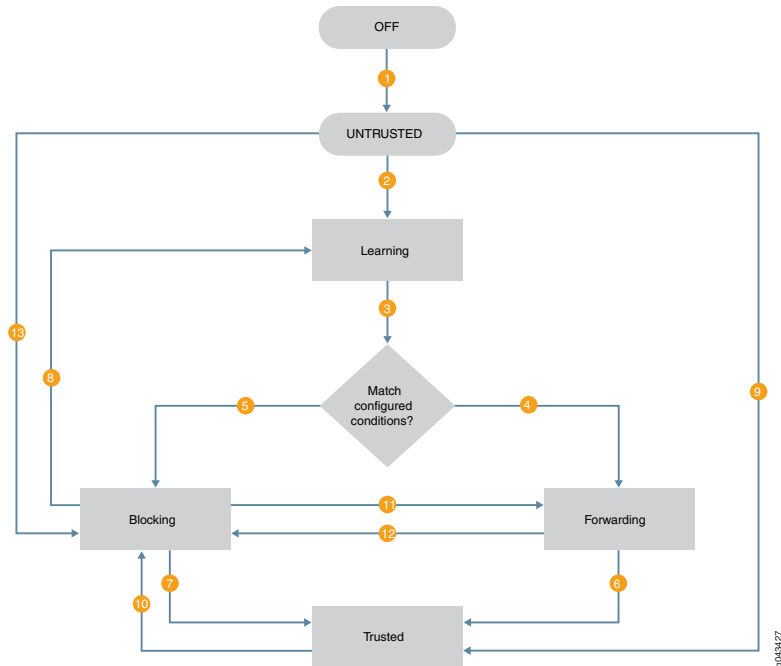
[Table 31 on page 512](#) summarizes the states of IPv6 RA guard for both stateless and stateful mode.

Table 31: IPv6 RA guard states

State	Description	Mode
Off	The interface operates as if RA guard is not available.	Stateless/stateful
Untrusted	The interface forwards ingress RA messages if received RA messages are validated against the configured policy rules; otherwise, it drops the RA message. Untrusted state is the default state of an interface enabled for RA guard.	Stateless/stateful
Blocked	The interface blocks ingress RA messages.	Stateless/stateful
Forwarding	The interface forwards ingress RA messages if received RA messages are validated against the configured policy rules; otherwise, it drops the RA messages.	Stateful
Learning	The switch actively acquires information about the IPv6 routing device connected to the interface. The learning process takes place over a predefined period of time.	Stateful
Trusted	The interface forwards all RA messages directly, without validating them against the policy.	Stateless/stateful

Figure 36 on page 513 illustrates the transition of states when stateful RA guard is enabled. The numbers shown on the illustrations are described in the text that follows; these are not sequential steps.

Figure 36: Stateful RA Guard State Transitions



1. When RA guard is enabled on an interface it moves to the *untrusted* state from the *off* state. The *untrusted* state is the default state of an interface that is enabled for RA guard.
2. When the command requesting the learning state is issued, the interface is moved from the *off* state to the *learning* state.
3. RA messages received during the learning state are compared to the configured policy.
4. If RA messages are validated against the configured policy, the interface moves to *forwarding* state.
5. If RA messages are not validated against the configured policy, the interface moves to *blocked* state.
6. If **mark-interface trust** is configured on the validated interface, then it moves from *forwarding* state to *trusted* state.
7. If **mark-interface trust** is configured on the blocked interface, then it moves from *blocked* state to *trusted* state.
8. If learning is requested on a blocked interface, then the interface moves from the *blocked* state to the *learning* state.

9. If an interface in the default *untrusted* state is configured as **mark-interface trust**, it moves directly to the trusted state. In this case a policy can not be applied on that interface.
10. If the **mark-interface trust** configuration is deleted, and no valid RAs are received on the interface, then the interface moves to the *blocked* state.
11. If the command requesting the forwarding state is issued, then the interface moves directly from *blocked* to *forwarding* state.
12. If the command requesting the blocking state is issued, then the interface moves directly from *forwarding* to *blocked*.
13. If an interface in the default *untrusted* state is configured as **mark-interface block**, it moves directly to the *blocked* state. In this case a policy can not be applied on that interface.

**Related
Documentation**

- [IPv6 Neighbor Discovery Protocol Overview](#)
- [Port Security Features on page 3](#)
- [Configuring Port Security \(non-ELS\) on page 11](#)

Configuring Stateful IPv6 Router Advertisement Guard

Stateful IPv6 Router Advertisement (RA) guard enables a switch to learn about the sources of RA messages for a certain period of time. During this period, during which the switch is known to be in the learning state, the information contained in received RA message attributes is stored and compared to the policy. At the end of the learning period, the switch has a record of which interfaces are attached to links with valid IPv6 routers. If there is no valid IPv6 router attached to an interface, the switch dynamically transitions the interface from the learning state into the blocking state. Subsequent RA messages received after the transition to blocking state are dropped. If there is a valid IPv6 router attached to the interface, the interface transitions to the forwarding state. In the forwarding state, RA messages that can be validated against the configured policy are forwarded.

You can override the dynamic state transitions by statically configuring the forwarding or blocking states on an interface. When you statically configure the state on an interface, the state can be changed only through configuration. For example, if you configure the forwarding state on an interface, the interface remains in the forwarding state until you configure a different state on that interface.

Before you can enable IPv6 RA guard on an interface or a VLAN, you must configure a policy. Stateful RA guard uses the policy to determine whether the RA messages received on an interface are from valid senders. You can configure the policy to either accept or discard RA messages that meet the predefined criteria. If the criteria for the policy includes

source addresses or address prefixes, you must configure a list of the addresses before configuring the policy.

- [Enabling Stateful RA Guard on an Interface on page 515](#)
- [Enabling Stateful RA Guard on a VLAN on page 515](#)
- [Configuring the Learning State on an Interface on page 516](#)
- [Configuring the Forwarding State on an Interface on page 517](#)
- [Configuring the Blocking State on an Interface on page 517](#)

Enabling Stateful RA Guard on an Interface

You can enable stateful RA guard on an interface. You must first configure a policy, which is used to validate incoming RA messages during the learning period. After you apply an RA guard policy to an interface, you must enable RA guard on the corresponding VLAN.

To enable stateful RA guard on an interface:

1. Apply a policy to an interface.

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard interface
interface-name policy policy-name
```

2. Configure the **stateful** option on the interface:

```
[edit forwarding-options access-security router-advertisement-guard interface
interface-name policy policy-name]
user@switch# set stateful
```

3. Enable stateful RA guard on the corresponding VLAN:

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard vlans
vlan-name policy policy-name stateful
```

Enabling Stateful RA Guard on a VLAN

You can enable stateful RA guard on a per-VLAN basis or for all VLANs. You must first configure a policy, which used to validate incoming RA messages during the learning state.

To enable stateful RA guard on a specific VLAN:

1. Apply a policy to a VLAN.

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard vlans
vlan-name policy policy-name
```

2. Configure the **stateful** option on the VLAN:

```
[edit forwarding-options access-security router-advertisement-guard vlans
vlan-name policy policy-name]
```

```
user@switch# set stateful
```

To enable stateful RA guard on all VLANs:

1. Apply a policy to all VLANs.

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard vlans all
policy policy-name
```



NOTE: If a policy has been configured for a specific VLAN using the command `set forwarding-options access-security router-advertisement-guard vlans vlan-name policy policy-name`, that policy takes priority over the policy applied globally to all VLANs.

2. Configure the **stateful** option on all VLANs:

```
[edit forwarding-options access-security router-advertisement-guard vlans all
policy policy-name]
user@switch# set stateful
```

Configuring the Learning State on an Interface

When stateful RA guard is first enabled, the default state is *off*. An interface in the off state operates as if RA guard is not available. To transition an interface to the learning state, you must request learning on the interface. An interface in the learning state actively acquires information from the RA messages that it receives.

To configure stateful RA guard learning on an interface:

1. Request learning on the interface.

```
[edit]
user@switch# request access-security router-advertisement-guard-learn interface
interface-name
```

2. Configure the learning period in seconds.

```
[edit]
user@switch# request access-security router-advertisement-guard-learn interface
interface-name duration seconds
```

3. Configure the action to take on ingress RA messages received during the learning period. To forward RA messages received during the learning period, configure forwarding on the interface.

- To forward RA messages during the learning period:

```
[edit]
user@switch# request access-security router-advertisement-guard-learn interface
interface-name duration seconds forward
```


- To block RA messages during the learning period:

```
[edit]
user@switch# request access-security router-advertisement-guard-learn interface
interface-name duration seconds block
```

Configuring the Forwarding State on an Interface

An interface in the forwarding state accepts ingress RA messages that can be validated against the configured policy and forwards them to their destination. An interface can dynamically transition to the forwarding state directly from the learning state, or the forwarding state can be statically configured on the interface.

- To configure the forwarding state on an interface:

```
[edit]
user@switch# request access-security router-advertisement-guard-forward interface
interface-name
```

Configuring the Blocking State on an Interface

An interface in the blocking state blocks ingress RA messages. An interface can dynamically transition to the blocking state directly from the learning state, or the blocking state can be statically configured on the interface. An interface that has been statically configured to be in the blocking state will remain in the blocking state until another state is configured on that interface.

- To configure the blocking state on an interface:

```
[edit]
user@switch# request access-security router-advertisement-guard-block interface
interface-name
```

Related Documentation

- [Understanding IPv6 Router Advertisement Guard on page 511](#)
- [Configuring Stateless IPv6 Router Advertisement Guard on page 517](#)

Configuring Stateless IPv6 Router Advertisement Guard

Stateless IPv6 Router Advertisement (RA) guard enables the switch to examine incoming RA messages and filter them based on a predefined set of criteria. If the switch validates the content of the RA message, it forwards the RA message to its destination; otherwise, the RA message is dropped.

Before you can enable IPv6 RA guard, you must configure a policy with the criteria to be used for validating RA messages received on an interface. You can configure the policy to either accept or discard RA messages on the basis of whether they meet the criteria. The criteria are compared to information included in the RA messages. If the criteria for

the policy includes source addresses or address prefixes, you must configure a list of the addresses before configuring the policy.

- [Configuring a Discard Policy for RA Guard on page 518](#)
- [Configuring an Accept Policy for RA Guard on page 519](#)
- [Enabling Stateless RA Guard on an Interface on page 521](#)
- [Enabling Stateless RA Guard on a VLAN on page 522](#)
- [Configuring an Interface as Trusted or Blocked to Bypass Inspection by RA Guard on page 522](#)

Configuring a Discard Policy for RA Guard

You can configure a discard policy to drop RA messages from predefined sources. You must first configure a list or lists of the source addresses or address prefixes, and then associate them with a policy. The following lists can be associated with discard policy:

- **source-ip-address-list**
- **source-mac-address-list**
- **prefix-list-name**



NOTE: You can include more than one type of list in a discard policy. If the information contained in a received RA message matches any one of the list parameters, then that RA message is discarded.

To configure a discard policy for RA guard:

1. Define one or more lists of disallowed source addresses or address prefixes that RA guard will use to filter incoming RA messages. Add one address or address prefix per line in the configuration.

- To define a list of IPv6 source addresses:

```
[edit]
user@switch# set policy-options prefix-list address-list-name ipv6-address
```

- To define a list of IPv6 address prefixes:

```
[edit]
user@switch# set policy-options prefix-list prefix-list-name ipv6-prefix
```

- To define a list of MAC source addresses:

```
[edit]
user@switch# set policy-options mac-list address-list-name mac-address
```

2. Configure the policy name:

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard policy
policy-name
```

3. Specify the discard action:

```
[edit forwarding-options access-security router-advertisement-guard policy
policy-name]
user@switch# set discard
```

4. Associate the policy with the list or lists defined in Step 1. For example, to discard RA messages that match a source MAC address in the list:

```
[edit forwarding-options access-security router-advertisement-guard policy
policy-name discard]
user@switch# set source-mac-address-list address-list-name
```

Configuring an Accept Policy for RA Guard

You can configure an accept policy to forward RA messages on the basis of certain criteria. You can configure either match lists of source address or address prefixes as the criteria, or you can configure other match conditions, such as hop limit, configuration flags, or router preference as the criteria.

The following lists can be associated with an accept policy by using the **match-list** option:

- **source-ip-address-list**
- **source-mac-address-list**
- **prefix-list-name**



NOTE: You can associate more than one type of match list with an accept policy. If the **match-all** suboption is configured, then a received RA message must match all configured match lists in order to be forwarded; otherwise, it is discarded. If the **match-any** option is configured, then a received RA message must match any one of the configured match lists in order to be forwarded; if it does not match any of the configured lists, then it is discarded.

The following match conditions can be configured using the **match-option** option:

- **hop-limit**—Configure the RA guard policy to verify the minimum or maximum hop count for an incoming RA message.
- **managed-config-flag**—Configure the RA guard policy to verify that the managed address configuration flag of an incoming RA message is set.
- **other-config-flag**—Configure the RA guard policy to verify that the other configuration flag of an incoming RA message is set.
- **router-preference-maximum**—Configure the RA guard policy to verify that the default router preference parameter value of an incoming RA message is lower than or equal to a specified limit.



NOTE: The **match-list** and **match-option** options are used only in accept policies, not in discard policies.

To configure an accept policy for RA guard by using the **match-list** option:

1. Define one or more lists of authorized source addresses or address prefixes that RA guard will use to filter incoming RA messages. Add one address or address prefix per line in the configuration.

- To define a list of IPv6 source addresses:

```
[edit]
user@switch# set policy-options prefix-list address-list-name ipv6-address
```

- To define a list of IPv6 address prefixes:

```
[edit]
user@switch# set policy-options prefix-list prefix-list-name ipv6-prefix
```

- To define a list of MAC source addresses:

```
[edit]
user@switch# set policy-options mac-list address-list-name mac-address
```

2. Specify the policy name:

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard policy
policy-name
```

3. Specify the accept action:

```
[edit forwarding-options access-security router-advertisement-guard policy
policy-name]
user@switch# set accept
```

4. Specify whether RA guard must meet the criteria in all lists or in any of the lists configured in 1:

- To match on all lists:

```
[edit forwarding-options access-security router-advertisement-guard policy
policy-name accept]
user@switch# set match-list match-criteria match-all
```

- To match on any of the lists:

```
[edit forwarding-options access-security router-advertisement-guard policy
policy-name accept]
user@switch# set match-list match-criteria match-any
```

5. Associate the accept policy with the list or lists configured in Step 1. For example:

```
[edit forwarding-options access-security router-advertisement-guard policy
policy-name accept
user@switch# set match-list source-mac-address-list address-list-name
```

To configure an accept policy for RA guard using the **match-option** option:

1. Specify the policy name:

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard policy
policy-name
```

2. Specify the accept action:

```
[edit forwarding-options access-security router-advertisement-guard policy
policy-name]
user@switch# set accept
```

3. Specify the match conditions by using the **match-option** option. For example, to specify a match on the maximum number of hops:

```
[edit forwarding-options access-security router-advertisement-guard policy
policy-name accept]
user@switch# set match-option hop-limit maximum value
```

Enabling Stateless RA Guard on an Interface

You can enable stateless RA guard on an interface. You must first configure a policy, which is applied to incoming RA messages on the interface or interfaces. After you apply a policy to an interface, you must also enable RA guard on the corresponding VLAN; otherwise, the policy applied to the interface does not have any impact on received RA packets.

To enable stateless RA guard on an interface:

1. Apply a policy to an interface:

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard interface
interface-name policy policy-name
```

2. Configure the **stateless** option on the interface:

```
[edit forwarding-options access-security router-advertisement-guard interface
interface-name policy policy-name]
user@switch# set stateless
```

3. Enable stateless RA guard on the corresponding VLAN:

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard vlans
vlan-name policy policy-name stateless
```

Enabling Stateless RA Guard on a VLAN

You can enable stateless RA guard on a per-VLAN basis or for all VLANs. You must first configure a policy, which is used to validate incoming RA messages in the learning state.

To enable stateless RA guard on a specific VLAN:

1. Apply a policy to a VLAN.

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard vlans
vlan-name policy policy-name
```

2. Configure the **stateless** option on the VLAN:

```
[edit forwarding-options access-security router-advertisement-guard vlans
vlan-name policy policy-name]
user@switch# set stateless
```

To enable stateless RA guard on all VLANs:

1. Apply a policy to all VLANs.

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard vlans all
policy policy-name
```



NOTE: If a policy has been configured for a specific VLAN using the command `set forwarding-options access-security router-advertisement-guard vlans vlan-name policy policy-name`, that policy takes priority over the policy applied globally to all VLANs.

2. Configure the **stateful** option on all VLANs:

```
[edit forwarding-options access-security router-advertisement-guard vlans all
policy policy-name]
user@switch# set stateful
```

Configuring an Interface as Trusted or Blocked to Bypass Inspection by RA Guard

You can configure an interface as trusted or blocked to bypass inspection of RA messages by RA guard. When an RA message is received on a trusted or blocked interface, it is not subject to validation against the configured policy. A trusted interface forwards all RA messages. A blocked interface discards all RA messages.

- To configure an interface as trusted:

```
[edit]
user@switch# set forwarding-options access-security router-advertisement-guard interface
interface-name mark-interface trusted
```

- To configure an interface as blocked:

[edit]

```
user@switch# set forwarding-options access-security router-advertisement-guard interface  
interface-name mark-interface block
```

**Related
Documentation**

- [Understanding IPv6 Router Advertisement Guard on page 511](#)
- [Configuring Stateful IPv6 Router Advertisement Guard on page 514](#)

PART 9

Distributed Denial-of-Service (DDoS) Protection

- [DDoS Protection on page 527](#)

CHAPTER 22

DDoS Protection

- [Distributed Denial-of-Service \(DDoS\) Protection Overview on page 527](#)
- [Configuring DDoS Protection on page 535](#)
- [Tracing DDoS Protection Operations on page 543](#)
- [Example: Configuring DDoS Protection on page 546](#)
- [Example: Configuring DDoS Protection on QFX Series Switches on page 556](#)
- [Rate Limiting ICMPv4 and ICMPv6 Traffic on page 560](#)

Distributed Denial-of-Service (DDoS) Protection Overview

A denial-of-service (DoS) attack is any attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. Distributed denial-of-service (DDoS) attacks involve an attack from multiple sources, enabling a much greater amount of traffic to attack the network. The attacks typically use network protocol control packets to trigger a large number of exceptions to the device's control plane. This results in an excessive processing load that disrupts normal network operations.

Junos OS DDoS protection enables the device to continue functioning while under an attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. A single point of DDoS protection management enables network administrators to customize profiles for their network control traffic. For routers, protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases.

Host-bound Traffic Policers for DDoS Violations

To protect against DDoS attacks, you can configure policers for host-bound traffic. Host-bound traffic is traffic destined to the Routing Engine, including protocol control packets for routing protocols, such as OSPF and BGP. Traffic destined to router IP addresses is also considered host-bound traffic.

The policers specify rate limits for all control traffic for a given protocol, or, in some cases, for specific control packet types for a protocol. You can monitor policer actions for packet types and protocol groups at the level of the device, Routing Engine, and line cards. You can also control logging of policer events.

Control traffic is dropped when it exceeds any configured policer values or, for unconfigured policers, the default policer values. When a DDoS violation is reached, the device will not stop processing packets; it only limits their rate. Each violation immediately generates a notification to alert operators about a possible attack. The violation is counted, the time that the violation starts is noted, and the time of the last observed violation is noted. When the traffic rate drops below the bandwidth violation threshold, a recovery timer determines when the traffic flow is considered to have returned to normal. If no further violation occurs before the timer expires, the violation state is cleared and a notification is generated.



NOTE: On PTX routers and QFX Series switches, the timer is set to 300 seconds and cannot be modified.

The first line of protection is the policer on the Packet Forwarding Engine (PFE). On devices with multiple line cards, policer states and statistics from each line card are relayed to the Routing Engine and aggregated. The policer states are maintained during a switchover. Although line card statistics and violation counts are preserved during a switchover, Routing Engine policer statistics are not. Control traffic arriving from all ports of the line card converges on the Packet Forwarding Engine, where it is subject to policing. Thus, excess packets are dropped before they reach the Routing Engine, ensuring that the Routing Engine receives only the amount of traffic it can process.

On QFX Series switches and PTX Series routers, the DDoS policers operate at the PFE and line card level only.

In addition to providing notification of violations through event logging, Junos OS DDoS protection allows you to monitor policers, obtaining information such as policer configuration, number of violations encountered, date and time of violations, packet arrival rates, and number of packets received or dropped.



NOTE: DDoS protection policers act on the system's traffic queues. The QFX5100 and QFX5200 lines of switches manage traffic for more protocols than the number of queues, so the system often must map more than one protocol to the same queue. When traffic for one protocol shares a queue with other protocols and violates DDoS protection policer limits, these devices report a violation on that queue for all mapped protocols because the system doesn't distinguish which protocol's traffic specifically caused the violation. You can use what you know about the types of traffic flowing through your network to identify which of the reported protocols actually triggered the violation.

Platform Support

In Junos OS Release 14.2 and later releases, DDoS protection is supported on specific platforms. Verify that your installation includes any of the following:

- EX9200 switches.
- MX Series routers that have only MPCs installed: MX240, MX480, MX960, MX2010, and MX2020.
- MX Series routers with a built-in MPC: MX5, MX10, MX40, MX80, and MX104.



NOTE: For simplicity, where the text refers to line cards or line card policers, for these routers that means the built-in MPC.

Because these routers do not have FPC slots, information displayed in FPC fields by `show` commands actually refers to TFEB.

- PTX Series routers that have only PE-based FPCs installed (PTX3000, PTX5000, PTX1000, and PTX10000) support DDoS protection starting in Junos OS Release 17.4R1.

PTX10002 routers support DDoS protection starting in Junos OS Release 18.2R1.

- QFX Series switches, including the QFX5100 line, QFX5200 line, and the QFX10000 line of switches.

QFX10002-60C switches support DDoS protection starting in Junos OS Release 18.1R1.

- T4000 routers that have only Type 5 FPCs installed.



NOTE:

- For router platforms that have other line cards in addition to MPCs (MX Series), Type 5 FPCs (T4000), or PE-based FPCs (PTX3000, PTX5000, PTX1000, and PTX10000), the CLI accepts the configuration but the other line cards are not protected, so the router is not protected.
- DDoS protection support for Enhanced Subscriber Management was added in Junos OS Release 17.3R1 on routing platforms.
- To configure DDoS protection for supported protocol groups and packet types, PTX Series routers and QFX Series switches have CLI configuration options that differ significantly from the options available for MX Series and T4000 routers. See [protocols \(DDoS\) \(PTX Series and QFX Series\)](#) for the available DDoS protection configuration options on PTX routers and QFX Series switches.

Policer Types and Packet Priorities

DDoS protection includes two types of policers:

- An *aggregate policer* is applied to the complete set of packet types that belong to a protocol group. For example, you can configure an aggregate policer that applies to all PPPoE control packet types or to all DHCPv4 control packet types. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority for aggregate policers. An aggregate policer is supported by all protocol groups.
- An *individual policer*, also referred to as a *packet-type policer*, is allocated for each control packet type within a protocol group. For example, you can configure a policer for one or more types of PPPoE control packets, RADIUS control packets, or multicast snooping packets. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority for packet-type policers. Individual policers are available for some protocol groups.

Protocol group and packet type support varies across platforms and Junos OS releases, as follows:

- For routing devices except PTX Series routers, see [protocols \(DDoS\)](#).
- For PTX Series routers and QFX Series switches, see [protocols \(DDoS\) \(PTX Series and QFX Series\)](#).

A control packet is policed first by its individual policer (if supported) and then by its aggregate policer. A packet dropped by the individual policer never reaches the aggregate policer. A packet that passes the individual policer can subsequently be dropped by the aggregate policer.

Packet types within a protocol group have a default, configurable priority: low, medium, or high. Each control packet competes with other packets for the bandwidth within the limit imposed by its aggregate policer based on the priority configured for each packet type in the protocol group.

The priority mechanism is absolute. High-priority traffic gets bandwidth in preference to medium-priority and low-priority traffic. Medium-priority traffic gets bandwidth in preference to low-priority traffic. Low-priority traffic can use only the bandwidth left by high-priority and medium-priority traffic. If higher priority traffic takes all of the bandwidth, then all the lower priority traffic is dropped.

Example of Policer Priority Behavior

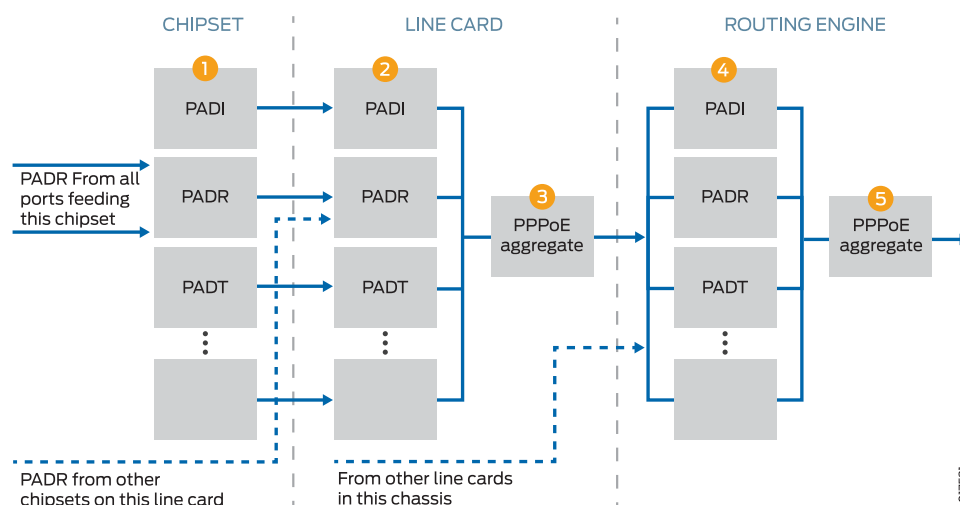
For example, on a device that supports DDoS protection for the PPPoE protocol group, consider how you might configure packet types within this protocol group. Ignoring other PPPoE packet types for this example, suppose you configure individual policers for PADI and PADT packets, as well as a PPPoE aggregate policer for all those packets. You prioritize PADT packets over PADI packets because PADT packets enable the PPPoE application to release resources to accept new connections. Therefore, you assign high priority to the PADT packets and low priority to the PADI packets.

The aggregate policer imposes a total bandwidth limit for the protocol group. PADT packets passed by their individual policer have access to that bandwidth before PADI packets passed by their individual policer, because the PADT packets have a higher priority. If so many PADT packets are passed that they use all the available bandwidth, then all the PADI packets are dropped, because there is no bandwidth remaining at the aggregate policer.

Policer Hierarchy on Routers

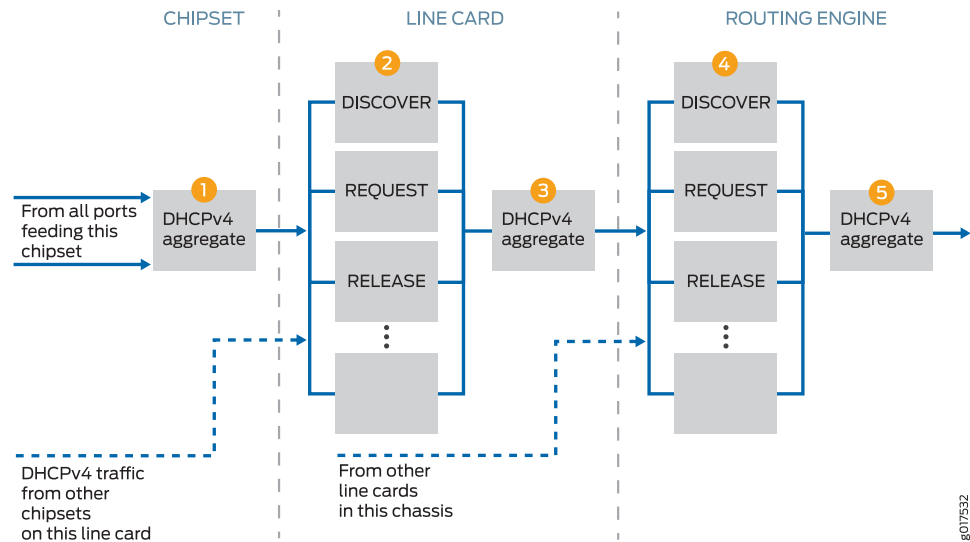
DDoS policers are organized to match the hierarchical flow of protocol control traffic. Control traffic arriving from all ports of a line card converges on the Packet Forwarding Engine. Control traffic from all line cards on the router converges on the Routing Engine. Similarly, the DDoS policers are placed hierarchically along the control paths so that excess packets are dropped as early as possible on the path. This design preserves system resources by removing excess, malicious traffic so that the Routing Engine receives only the amount of traffic that it can process. To implement this design, typically five DDoS policers are present: One on the Packet Forwarding Engine (the chipset), two at the line card, and two at the Routing Engine. An aggregate policer is also present on the Packet Forwarding Engine for some protocol groups, for a total of six policers; for simplicity, the text follows the general case. For example, [Figure 37 on page 531](#) shows the policer process for PPPoE traffic. [Figure 38 on page 532](#) shows the policer process for DHCPv4 traffic. (The same process applies to DHCPv6 traffic as well.)

Figure 37: Policer Hierarchy for PPPoE Packets



8017531

Figure 38: Policer Hierarchy for DHCPv4 Packets



g017532

Control packets arrive at the Packet Forwarding Engine for processing and forwarding. The first policer (1) is either an individual policer (Figure 37 on page 531) or an aggregate policer (Figure 38 on page 532).

- The first policer is an individual policer for protocol groups that support individual policers, with two exceptions. For DHCPv4 and DHCPv6 traffic, the first policer is an aggregate policer.
- The first policer is an aggregate policer for protocol groups that support only aggregate policers.

Traffic that passes the first policer is monitored by one or both of the line card policers. If the card has more than one Packet Forwarding Engine, traffic from all Packet Forwarding Engines converges on the line card policers.

- When the traffic belongs to a protocol group that supports individual policers, it passes through the line card individual policer (2) and then the line card aggregate policer (3). Traffic that passes the individual policer can be dropped by the aggregate policer. Although DHCPv4 and DHCPv6 traffic was monitored by an aggregate policer at the Packet Forwarding Engine, at the line card it is handled like other protocols that support individual policers.
- When the traffic belongs to a protocol group that supports only aggregate policers, only the line card aggregate policer monitors the traffic.

Traffic that passes the line card policers is monitored by one or both of the Routing Engine policers. Traffic from all the line cards converges on the Routing Engine policers.

- When the traffic belongs to a protocol group that supports individual policers, it passes through the Routing Engine individual policer (4) and then the Routing Engine aggregate policer (5). Traffic that passes the individual policer can be dropped by the aggregate

policer. As it was at the line card level, DHCPv4 and DHCPv6 traffic at the Routing Engine is handled like other protocols that support individual policers.

- When the traffic belongs to a protocol group that supports only aggregate policers, only the aggregate policer monitors the traffic.

With this design, three policers evaluate the traffic for protocol groups that support only aggregate policers. Among other groups, this includes ANCP, dynamic VLAN, FTP, and IGMP traffic. Traffic for protocol groups that support both aggregate and individual policers is evaluated by all five policers. Among other groups, this includes DHCPv4, MLP, PPP, PPPoE, and virtual chassis traffic.

Figure 37 on page 531 shows how DDoS protection polices PPPoE control packets:

1. PADR packets, for example, are evaluated at the first policer on the Packet Forwarding Engine to determine whether they are within the bandwidth limits. PADR packets that exceed the limit are dropped.
2. All PADR packets that pass the policer on all Packet Forwarding Engines on the line card are next evaluated by the line card individual policer. PADR packets that exceed the limit are dropped.
3. All PADR packets that pass the line card individual policer proceed to the line card aggregate policer. PADR packets that exceed the limit are dropped.
4. All PADR packets that are passed by the line card aggregate policers on all line cards on the router proceed to the Routing Engine individual policer. PADR packets that exceed the limit are dropped.
5. Finally, all PADR packets that are passed by the Routing Engine individual policer proceed to the Routing Engine aggregate policer. PADR packets that exceed the limit are dropped. PADR packets that are not dropped here are passed along as safe, normal traffic.

By default, all three individual policers (Packet Forwarding Engine, line card, and Routing Engine) have the same bandwidth limit for a given packet type. This design enables all the control traffic from a Packet Forwarding Engine and line card to reach the Routing Engine, as long as there is no competing traffic of the same type from other Packet Forwarding Engines or line cards. When competing traffic is present, excess packets are dropped at the convergence points. That is, they are dropped at the line card for all competing Packet Forwarding Engines and at the Routing Engine for all competing line cards.

Example of Policer Bandwidth Limit Behavior

For example, suppose you set the policer bandwidth for PADI packets to 1000 packets per second. This value applies to the individual PADI policers at the Packet Forwarding Engine, the line card, and the Routing Engine. If only the card in slot 5 is receiving PADI packets, then up to 1000 PADI pps can reach the Routing Engine (if the PPPoE aggregate policer is not exceeded). However, suppose the card in slot 9 is also receiving PADI packets at 1000 pps and that its PPPoE aggregate policer is not exceeded. The traffic passes the individual and aggregate policers at both line cards and proceeds to the Routing Engine. At the Routing Engine, the combined bandwidth is 2000 pps. Because the PADI policer

at the Routing Engine allows only 1000 PADI pps to pass, it drops the excess 1000 packets. It continues to drop the excess packets for as long as the bandwidth is exceeded.

You can apply a scaling factor for both the bandwidth limit and the burst limit at the line card. This enables you to fine-tune the traffic limits for each slot. For example, suppose the individual policer sets the PADI packet bandwidth to 1000 pps and the burst size to 50,000 packets. You can reduce the traffic limit for PADI packets on any line card by specifying the slot number and scaling factor. A bandwidth scaling factor of 20 for slot 5 reduces the traffic in this example to 20 percent of 1000 pps, or 200 pps for the line card in that slot. Similarly, a burst scaling factor of 50 for that slot reduces the burst size by 50 percent to 25,000 packets. By default, scaling factors are set to 100 so traffic can pass through at 100 percent of the rate limit.

DDoS Protection Compared to Subscriber Login Packet Overload Protection

In addition to the DDoS protection capability, MX Series routers also have a built-in subscriber login overload protection mechanism. The login overload protection mechanism (also called a load-throttling mechanism) monitors the incoming subscriber login packets and admits only what the system is capable of handling in accordance with the prevailing load on the system. Packets in excess of what the system can handle are discarded. By shedding this excess load, the system is able to maintain optimal performance and prevent any degradation of login-completion rate under overload conditions. This mechanism uses minimal resources and is enabled by default; no user configuration is required.

The protection provided by this mechanism is secondary to what DDoS protection provides as a first level of defense against high rates of incoming packets. DDoS protection operates on the Packet Forwarding Engine and protects against all packet types of all protocols. In contrast, the login overload protection mechanism is located on the Routing Engine and specifically operates only on incoming connection-initiation packets such as DHCPv4 DHCPDISCOVER, DHCPv6 SOLICIT, and PPPoE PADI packets.

Release History Table

Release	Description
18.2R1	PTX10002 routers support DDoS protection starting in Junos OS Release 18.2R1.
18.2R1	QFX10002-60C switches support DDoS protection starting in Junos OS Release 18.1R1.
17.4R1	PTX Series routers that have only PE-based FPCs installed (PTX3000, PTX5000, PTX1000, and PTX10000) support DDoS protection starting in Junos OS Release 17.4R1.
17.3R1	DDoS protection support for Enhanced Subscriber Management was added in Junos OS Release 17.3R1 on routing platforms.
14.2	In Junos OS Release 14.2 and later releases, DDoS protection is supported on specific platforms.

**Related
Documentation**

- [Configuring DDoS Protection on page 535](#)
- [DDoS Protection Flow Detection Overview on page 565](#)

Configuring DDoS Protection

DDoS protection is enabled by default for all supported protocol groups and packet types. Default values are present for bandwidth, bandwidth scale, burst, burst scale, priority, and recover time. You can change the DDoS configuration for individual packet types supported within a protocol group or for the aggregate policer for the protocol group.

DDoS logging is enabled by default, but you can disable it globally for all DDoS events or for individual packet types within a protocol group. You can also fine-tune monitoring of DDoS events by configuring tracing operations.

On routing devices, you can disable DDoS protection at the Routing Engine and for all line cards either globally or for individual packet types within a protocol group. On PTX Series routers and QFX Series switches, policers are supported only at the line cards; you can disable DDoS protection for all line cards globally or for individual packet types.



NOTE: MX Series routers with MPCs and T4000 routers with FPC5s support DDoS protection. The CLI accepts the configuration if other line cards are also installed on either of these types of routers, but the other line cards are not protected so the router is essentially not protected.

To configure DDoS protection:

1. (Optional) Configure global DDoS protection settings or disable DDoS protection.

2. (Optional) Configure DDoS protection settings for the aggregate policer or individual packet types for the desired protocol groups.
 3. (Optional) Configure tracing for DDoS protection operations.
- [Disabling DDoS Protection Policers and Logging Globally on page 536](#)
 - [Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537](#)
 - [Verifying and Managing DDoS Protection on page 542](#)

Disabling DDoS Protection Policers and Logging Globally

DDoS policers are enabled by default for all supported protocol groups and packet types.

On MX Series routers, T4000 routers, and EX9200 switches, policers are established at the level of the individual line card and the Routing Engine. You can disable the line card policers globally for all MPCs or FPC5s. You can also disable the Routing Engine policer. When you disable either of these policers, the policers at that level for all protocol groups and packet types are disabled.

On PTX Series routers and QFX Series switches, policers are established at the level of individual line cards only. If you disable line-card policers globally, DDoS protection is disabled on the switch.

DDoS logging is also enabled by default. You can disable all DDoS event logging (including flow detection event logging) for all protocol groups and packet types across the router or switch.



NOTE: The global configuration for disabling policers and logging overrides any local configuration for packet types.

To configure global DDoS settings:

1. (Optional) To disable line card policers:

```
[edit system ddos-protection global]
user@host# set disable-fpc
```

2. (Optional) (Not available on PTX Series Routers or QFX Series switches) To disable Routing Engine policers:

```
[edit system ddos-protection global]
user@host# set disable-routing-engine
```

3. (Optional) To disable event logging:

```
[edit system ddos-protection global]
user@host# set disable-logging
```

Configuring DDoS Protection Aggregate or Individual Packet Type Policers

DDoS policers are applied to control packet traffic. You can configure the maximum allowed traffic rate, maximum burst size, traffic priority, and how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack. You can also scale the bandwidth and burst values for individual line cards so that the policers at this level trigger at lower thresholds than the overall protocol or packet thresholds.

Protocol group and packet type support varies across platforms and Junos OS releases, as follows:

- For most routing devices, see [protocols \(DDoS\)](#).
- For PTX Series routers and QFX Series switches, see [protocols \(DDoS\) \(PTX Series and QFX Series\)](#).

You can configure an aggregate policer for any protocol group. The aggregate policer applies to the combination of all types of control packet traffic for that group. For some protocol groups, you can also configure policers for individual packet types. When you configure an aggregate policer for certain protocol groups, you can optionally bypass that policer for one or more particular packet types in that group.

DDoS protection is enabled by default. Although all policers have default parameter values, these values might not accurately reflect the control traffic pattern of your network.



BEST PRACTICE: We recommend that you model your network to determine the best values for your situation. Before you configure policers for your network, you can quickly view the default values for all packet types from operational mode using the `show ddos-protection protocols parameters brief` command. You can also use the command to specify a single protocol group of interest. For example, to see default values for the dhcpv4 protocol group, use the `show ddos-protection protocols dhcpv4 parameters brief` command.

You can disable a packet type policer at either the Routing Engine (if supported), at a specified line card, or for all line cards. You can also disable logging of all DDoS events for individual packet types within a protocol group.

To configure the desired aggregate or packet-type DDoS protection policer settings:

1. Specify the protocol group.

```
[edit system ddos-protection protocols]
user@host# edit protocol-group
```

For example, to specify the DHCPv4 protocol group:

```
[edit system ddos-protection protocols]
user@host# edit dhcpv4
```

or, on PTX Series or QFX Series devices, DDoS protection support has a combined DHCPv4 and DHCPv6 option that allows only aggregate policer configuration:

```
[edit system ddos-protection protocols]
user@host# edit dhcpv4v6
```

2. Specify an individual packet type or the **aggregate** option to encompass all packet types in the protocol group.

```
[edit system ddos-protection protocols protocol-group]
user@host# set packet-type
```

or

```
[edit system ddos-protection protocols protocol-group]
user@host# set aggregate
```

For example, to specify the DHCPv4 release packets on devices that support individual DHCPv4 packet types:

```
[edit system ddos-protection protocols dhcpv4]
user@host# edit release
```

3. (Optional) Configure the maximum traffic rate the policer allows for the packet type (or aggregate).

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
user@host# set bandwidth packets-per-second
```

For example, to set a bandwidth of 600 packets per second for DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set bandwidth 600
```

4. (Optional) Configure the maximum number of packets of this packet type (or aggregate) that the policer allows in a burst of traffic.

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
user@host# set burst size
```

For example, to set a maximum of 5000 DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set burst 5000
```

5. (Optional) Set the traffic priority.

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
```

```
user@host# set priority level
```

For example, to specify a medium priority for DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set priority medium
```

6. (Optional) Configure how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack.

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
user@host# set recover-time seconds
```

For example, to specify that 600 seconds must have passed since the last violation of the DHCPv4 release packet policer:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set recover-time 600
```

7. (Optional, supported on some devices) Bypass the aggregate policer configuration. This is applicable only when an aggregate policer and an individual policer is configured for the protocol group.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set bypass-aggregate
```

For example, to bypass the aggregate policer for DHCPv4 renew packets:

```
[edit system ddos-protection protocols dhcpv4 renew]
user@host# set bypass-aggregate
```

8. (Optional) Disable line card policers for the packet type (or aggregate) on all line cards.

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
user@host# set disable-fpc
```



NOTE: When you disable line card policers globally at the [edit system ddos-protection global] hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

For example, to disable the line card policer for DHCPv4 bootp packets:

```
[edit system ddos-protection protocols dhcpv4 bootp]
user@host# set disable-fpc
```

9. (Optional) Disable DDoS event logging for only one packet type (or aggregate).

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
user@host# set disable-logging
```



NOTE: Events disabled for the packet are associated with policer violations; logging of flow detection culprit flow events is not affected by this statement.



NOTE: When you disable DDoS event logging globally at the [edit system ddos-protection global] hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

For example, to disable DDoS event logging on the line card policer for DHCPv4 discover packets:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set disable-logging
```

10. (Optional, if Routing Engine policers are supported) Disable the Routing Engine policer for only this packet type.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set disable-routing-engine
```



NOTE: When you disable the Routing Engine policer globally at the [edit system ddos-protection global] hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

For example, to disable the Routing Engine policer for DHCPv4 discover packets:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set disable-routing-engine
```

11. (Optional) Configure packet-level settings for the packet type (or aggregate) on a single line card. On switches with a single, fixed line card (a single FPC considered to be in slot 0 and labeled **fpc0**), scaling the policer values affects the entire switch.

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
user@host# edit fpc slot-number
```


For example, to access DHCPv4 discover packet settings on the line card in slot 3:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit fpc 3
```

12. (Optional) Scale the policer bandwidth for the packet type (or aggregate) on the line card.

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type) fpc
slot-number]
user@host# set bandwidth-scale percentage
```

For example, to scale the bandwidth to 80 percent of the all-line-card setting configured for DHCPv4 discover packets on the line card in slot 3:

```
[edit system ddos-protection protocols dhcpv4 discover fpc 3]
user@host# edit bandwidth-scale 80
```

13. (Optional) Scale the policer burst size for the packet type (or aggregate) on the line card.

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type) fpc
slot-number]
user@host# set burst-scale percentage
```

For example, to scale the maximum bandwidth to 75 percent of the all-line-card setting configured for DHCPv4 discover packets on the line card in slot 3:

```
[edit system ddos-protection protocols dhcpv4 discover fpc 3]
user@host# edit burst-scale 75
```

14. (Optional) Disable the line card policer for the packet type (or aggregate) on a particular line card.

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type) fpc
slot-number]
user@host# set disable-fpc
```

For example, to disable the line card policer for DHCPv4 discover packets on the line card in slot 3:

```
[edit system ddos-protection protocols dhcpv4 discover fpc 3]
user@host# edit disable-fpc
```

- See Also**
- [Example: Configuring DDoS Protection on page 546](#)
 - [Example: Configuring DDoS Protection on QFX Series Switches on page 556](#)

Verifying and Managing DDoS Protection

Purpose View or clear information about DDoS configurations, states, and statistics.

- Action**
- To display the DDoS policer configuration, violation state, and statistics for all packet types in all protocol groups:

```
user@host> show ddos-protection protocols
```

If you issue the command before you make any configuration changes, the default policer values are displayed.

- To display the DDoS policer configuration, violation state, and statistics for a particular packet type in a particular protocol group:

```
user@host> show ddos-protection protocols protocol-group packet-type
```

- To display only the number of DDoS policer violations for all protocol groups:

```
user@host> show ddos-protection protocols violations
```

- To display a table of the DDoS configuration for all packet types in all protocol groups:

```
user@host> show ddos-protection protocols parameters brief
```

- To display a complete list of packet statistics and DDoS violation statistics for all packet types in all protocol groups:

```
user@host> show ddos-protection protocols statistics detail
```

- To display global DDoS violation statistics:

```
user@host> show ddos-protection statistics
```

- To display the DDoS version number:

```
user@host> show ddos-protection version
```

- To clear DDoS statistics for all packet types in all protocol groups:

```
user@host> clear ddos-protection protocols statistics
```

- To clear DDoS statistics for all packet types in a particular protocol group:

```
user@host> clear ddos-protection protocols protocol-group statistics
```

- To clear DDoS statistics for a particular packet type in a particular protocol group:

```
user@host> clear ddos-protection protocols protocol-group packet-type statistics
```

- To clear DDoS violation states for all packet types in all protocol groups:

```
user@host> clear ddos-protection protocols states
```

- To clear DDoS violation states for all packet types in a particular protocol group:

```
user@host> clear ddos-protection protocols protocol-group states
```

- To clear DDoS violation states for a particular packet type in a particular protocol group:

```
user@host> clear ddos-protection protocols protocol-group packet-type states
```

See Also • [Verifying and Managing Flow Detection on page 575](#)

Tracing DDoS Protection Operations

The Junos OS trace feature tracks DDoS protection operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the `/var/log` directory. By default, the router uses the filename `jddosd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file *filename* reaches 128 kilobytes (KB), it is compressed and renamed *filename.0.gz*. Subsequent events are logged in a new file called *filename*, until it reaches capacity again. At this point, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the [System Log Explorer](#).)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

This topic describes how you can configure all aspects of DDoS tracing operations.

- [Configuring the DDoS Protection Trace Log Filename on page 544](#)
- [Configuring the Number and Size of DDoS Protection Log Files on page 544](#)
- [Configuring Access to the DDoS Protection Log File on page 544](#)
- [Configuring a Regular Expression for DDoS Protection Messages to Be Logged on page 545](#)

- [Configuring the DDoS Protection Tracing Flags on page 545](#)
- [Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged on page 545](#)

Configuring the DDoS Protection Trace Log Filename

By default, the name of the file that records trace output for DDoS protection is **jddosd**. You can specify a different name with the **file** option.

To configure the filename for subscriber management database tracing operations:

- Specify the name of the file used for the trace output.

```
[edit system ddos-protection traceoptions]  
user@host# set file ddos_logfile_1
```

Configuring the Number and Size of DDoS Protection Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format **.number.gz**. The newest archived file is **.0.gz** and the oldest archived file is **.(maximum number)-1.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, **filename**, reaches 2 MB, **filename** is compressed and renamed **filename.0.gz**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, **filename.19.gz**, is simply overwritten when the next oldest file, **filename.18.gz** is compressed and renamed to **filename.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

```
[edit system ddos-protection traceoptions]  
user@host# set file ddos_1_logfile_1 files 20 size 2097152
```

Configuring Access to the DDoS Protection Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1_logfile_1 world-readable
```

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1_logfile_1 no-world-readable
```

Configuring a Regular Expression for DDoS Protection Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events.

You can refine the output by including regular expressions to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1_logfile_1 match regex
```

Configuring the DDoS Protection Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system ddos-protection traceoptions]
user@host# set flag flag
```

Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages. By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

```
[edit system ddos-protection traceoptions]  
user@host# set level severity
```

See Also • [Tracing DDoS Protection Operations on page 543](#)

Example: Configuring DDoS Protection

This example shows how to configure DDoS protection that enables the router to quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources.

- [Requirements on page 546](#)
- [Overview on page 546](#)
- [Configuration on page 547](#)
- [Verification on page 549](#)

Requirements

DDoS protection requires the following hardware and software:

- MX Series routers that have only MPCs installed, T4000 Core Routers that have only FPC5s installed, EX9200 switches.



NOTE: If a router has other cards in addition to MPCs or FPC5s, the CLI accepts the configuration but the other cards are not protected and therefore the router is not protected.

- Junos OS Release 11.2 or later

No special configuration beyond device initialization is required before you can configure this feature.

Overview

Distributed denial-of-service attacks use multiple sources to flood a network or router with protocol control packets. This malicious traffic triggers a large number of exceptions in the network and attempts exhaust the system resources to deny valid users access to the network or server.

This example describes how to configure rate-limiting policers that identify excess control traffic and drop the packets before the router is adversely affected. Sample tasks include configuring policers for particular control packet types within a protocol group, configuring an aggregate policer for a protocol group and bypassing that policer for a particular control packet type, and specifying trace options for DDoS operations.

This example does not show all possible configuration choices.

Configuration

CLI Quick Configuration To quickly configure DDoS protection for protocol groups and particular control packet types, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
edit system
set ddos-protection protocols dhcpv4 aggregate bandwidth 669
set ddos-protection protocols dhcpv4 aggregate burst 6000
set ddos-protection protocols dhcpv4 discover bandwidth 100
set ddos-protection protocols dhcpv4 discover recover-time 200
set ddos-protection protocols dhcpv4 discover burst 300
set ddos-protection protocols dhcpv4 offer priority medium
set ddos-protection protocols dhcpv4 offer bypass-aggregate
set ddos-protection protocols dhcpv4 offer fpc 1 bandwidth-scale 80
set ddos-protection protocols dhcpv4 offer fpc 1 burst-scale 75
set ddos-protection protocols pppoe aggregate bandwidth 800
set ddos-protection traceoptions file ddos-trace size 10m
set ddos-protection traceoptions flag all
top
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure DDoS protection:

1. Specify a protocol group.

```
[edit system ddos-protection protocols]
user@host# edit dhcpv4
```

2. Configure the maximum traffic rate for the DHCPv4 aggregate policer; that is, for the combination of all DHCPv4 packets.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set aggregate bandwidth 669
```

3. Configure the maximum burst rate for the DHCPv4 aggregate policer.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set aggregate burst 6000
```

4. Configure the maximum traffic rate for the DHCPv4 policer for discover packets.

```
[edit system ddos-protection protocols dhcpv4]
```

```
user@host# set discover bandwidth 100
```

5. Decrease the recover time for violations of the DHCPv4 discover policer.

```
[edit system ddos-protection protocols dhcpv4]  
user@host# set discover recover-time 200
```

6. Configure the maximum burst rate for the DHCPv4 discover policer.

```
[edit system ddos-protection protocols dhcpv4]  
user@host# set discover burst 300
```

7. Increase the priority for DHCPv4 offer packets.

```
[edit system ddos-protection protocols dhcpv4]  
user@host# set offer priority medium
```

8. Prevent offer packets from being included in the aggregate bandwidth; that is, offer packets do not contribute towards the combined DHCPv4 traffic to determine whether the aggregate bandwidth is exceeded. However, the offer packets are still included in traffic rate statistics.

```
[edit system ddos-protection protocols dhcpv4]  
user@host# set offer bypass-aggregate
```

9. Reduce the bandwidth and burst size allowed before violation is declared for the DHCPv4 offer policer on the MPC or FPC5 in slot 1.

```
[edit system ddos-protection protocols dhcpv4]  
user@host# set offer fpc 1 bandwidth-scale 80  
user@host# set offer fpc 1 burst-scale 75
```

10. Configure the maximum traffic rate for the PPPoE aggregate policer, that is, for the combination of all PPPoE packets.

```
[edit system ddos-protection protocols dhcpv4]  
user@host# up  
[edit system ddos-protection protocols]  
user@host# set pppoe aggregate bandwidth 800
```

11. Configure tracing for all DDoS protocol processing events.

```
[edit system ddos-protection traceoptions]  
user@host# set file ddos-log  
user@host# set file size 10m  
user@host# set flag all
```


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

```
[edit system]
user@host# show ddos-protection
traceoptions {
  file ddos-trace size 10m;
  flag all;
}
protocols {
  pppoe {
    aggregate {
      bandwidth 800;
    }
  }
  dhcpv4 {
    aggregate {
      bandwidth 669;
      burst 6000;
    }
    discover {
      bandwidth 100;
      burst 300;
      recover-time 200;
    }
    offer {
      priority medium;
      fpc 1 {
        bandwidth-scale 80;
        burst-scale 75;
      }
      bypass-aggregate;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the DDoS protection configuration is working properly, perform these tasks:

- [Verifying the DHCPv4 DDoS Protection Configuration and Operation on page 549](#)
- [Verifying the PPPoE DDoS Configuration on page 553](#)

Verifying the DHCPv4 DDoS Protection Configuration and Operation

Purpose Verify that the DHCPv4 aggregate and protocol policer values have changed from the default. With DHCPv4 and PPPoE traffic flowing, verify that the policers are working correctly. You can enter commands to display the individual policers you are interested

in, as shown here, or you can enter the **show ddos-protection protocols dhcpv4** command to display this information for all DHCPv4 packet types.

Action From operational mode, enter the **show ddos-protection protocols dhcpv4 aggregate** command.

```
user@host> show ddos-protection protocols dhcpv4 aggregate
```

```
Protocol Group: DHCPv4
```

```
Packet type: aggregate (aggregate for all DHCPv4 traffic)
Aggregate policer configuration:
  Bandwidth:      669 pps
  Burst:          6000 packets
  Priority:        medium
  Recover time:   300 seconds
  Enabled:        Yes
System-wide information:
  Aggregate bandwidth is no longer being violated
  No. of FPCs currently receiving excess traffic: 0
  No. of FPCs that have received excess traffic: 1
  Violation first detected at: 2011-03-10 06:27:47 PST
  Violation last seen at:     2011-03-10 06:28:57 PST
  Duration of violation: 00:01:10 Number of violations: 1
  Received: 71064              Arrival rate: 0 pps
  Dropped: 23115              Max arrival rate: 1000 pps
Routing Engine information:
  Bandwidth: 669 pps, Burst: 6000 packets, enabled
  Aggregate policer is never violated
  Received: 36130              Arrival rate: 0 pps
  Dropped: 0                  Max arrival rate: 671 pps
  Dropped by aggregate policer: 0
FPC slot 1 information:
  Bandwidth: 100% (669 pps), Burst: 100% (5000 packets), enabled
  Aggregate policer is no longer being violated
  Violation first detected at: 2011-03-10 06:27:48 PST
  Violation last seen at:     2011-03-10 06:28:58 PST
  Duration of violation: 00:01:10 Number of violations: 1
  Received: 71064              Arrival rate: 0 pps
  Dropped: 34934              Max arrival rate: 1000 pps
  Dropped by individual policers: 11819
  Dropped by aggregate policer: 23115
```

From operational mode, enter the **show ddos-protection protocols dhcpv4 discover** command.

```
user@host> show ddos-protection protocols dhcpv4 discover
```

```
Protocol Group: DHCPv4
```

```
Packet type: discover (DHCPv4 DHCPDISCOVER)
Individual policer configuration:
  Bandwidth:      100 pps
  Burst:          300 packets
  Priority:        low
  Recover time:   200 seconds
  Enabled:        Yes
  Bypass aggregate: No
```

```

System-wide information:
  Bandwidth is no longer being violated
  No. of FPCs currently receiving excess traffic: 0
  No. of FPCs that have received excess traffic: 1
  Violation first detected at: 2011-03-10 06:28:34 PST
  Violation last seen at:      2011-03-10 06:28:55 PST
  Duration of violation: 00:00:21 Number of violations: 1
  Received: 47949                Arrival rate: 0 pps
  Dropped: 11819                 Max arrival rate: 671 pps
Routing Engine information:
  Bandwidth: 100 pps, Burst: 300 packets, enabled
  Policer is never violated
  Received: 36130                Arrival rate: 0 pps
  Dropped: 0                     Max arrival rate: 0 pps
  Dropped by aggregate policer: 0
FPC slot 1 information:
  Bandwidth: 100% (100 pps), Burst: 100% (300 packets), enabled
  Policer is no longer being violated
  Violation first detected at: 2011-03-10 06:28:35 PST
  Violation last seen at:      2011-03-10 06:28:55 PST
  Duration of violation: 00:00:20 Number of violations: 1
  Received: 47949                Arrival rate: 0 pps
  Dropped: 11819                 Max arrival rate: 671 pps
  Dropped by this policer: 11819
  Dropped by aggregate policer: 0

```

From operational mode, enter the **show ddos-protection protocols dhcpv4 offer** command.

```
user@host> show ddos-protection protocols dhcpv4 offer
```

```

Protocol Group: DHCPv4

Packet type: offer (DHCPv4 DHCPPOFFER)
Individual policer configuration:
  Bandwidth:      1000 pps
  Burst:          1000 packets
  Priority:        medium
  Recover time:   300 seconds
  Enabled:        Yes
  Bypass aggregate: Yes
System-wide information:
  Bandwidth is never violated
  Received: 0                Arrival rate: 0 pps
  Dropped: 0                 Max arrival rate: 0 pps
Routing Engine information:
  Policer is never violated
  Received: 0                Arrival rate: 0 pps
  Dropped: 0                 Max arrival rate: 0 pps
  Dropped by aggregate policer: 0
FPC slot 1 information:
  Bandwidth: 80% (800 pps), Burst: 75% (750 packets), enabled
  Policer is never violated
  Received: 0                Arrival rate: 0 pps
  Dropped: 0                 Max arrival rate: 0 pps
  Dropped by aggregate policer: 0

```

Meaning The output of these commands lists the policer configuration and traffic statistics for the DHCPv4 aggregate, discover, and offer policers respectively.

The **Aggregate policer configuration** section in the first output example and **Individual policer configuration** sections in the second and third output examples list the configured values for bandwidth, burst, priority, recover time, and bypass-aggregate.

The **System-wide information** section shows the total of all DHCPv4 traffic statistics and violations for the policer recorded across all line cards and at the Routing Engine. The **Routing engine information** section shows the traffic statistics and violations for the policer recorded at the Routing Engine. The **FPC slot 1 information** section shows the traffic statistics and violations for the policer recorded only at the line card in slot 1.

The output for the aggregate policer in this example shows the following information:

- The **System-wide information** section shows that 71,064 DHCPv4 packets of all types were received across all line cards and the Routing Engine. The section shows a single violation with a time stamp and that the aggregate policer at a line card dropped 23,115 of these packets.
- The **FPC slot 1 information** section shows that this line card received all 71,064 DHCPv4 packets, but its aggregate policer experienced a violation and dropped the 23,115 packets shown in the other section. The line card individual policers dropped an additional 11,819 packets.
- The **Routing Engine information** section shows that the remaining 36,130 packets all reached the Routing Engine and that its aggregate policer dropped no additional packets.

The difference between the number of DHCPv4 packets received and dropped at the line card $[71,064 - (23,115 + 11,819)]$ matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1 received any DHCPv4 packets.

The output for the DHCPv4 discover packet policer in this example shows the following information:

- The **System-wide information** section shows that 47,949 DHCPv4 discover packets were received across all line cards and the Routing Engine. The section shows a single violation with a time stamp and that the aggregate policer at a line card dropped 11,819 of these packets.
- The **FPC slot 1 information** section shows that this line card received all 47,949 DHCPv4 discover packets, but its individual policer experienced a violation and dropped the 11,819 packets shown in the other section.
- The **Routing Engine information** section shows that only 36,130 DHCPv4 discover packets reached the Routing Engine and that it dropped no additional packets.

The difference between the number of DHCPv4 discover packets received and dropped at the line card $(47,949 - 11,819)$ matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at

more than one line card. In this example, only the line card in slot 1 received any DHCPv4 discover packets.

The output for the DHCPv4 offer packet policer in this example shows the following information:

- This individual policer has never been violated at any location.
- No DHCPv4 offer packets have been received at any location.

Verifying the PPPoE DDoS Configuration

Purpose Verify that the PPPoE policer values have changed from the default.

Action From operational mode, enter the **show ddos-protection protocols pppoe parameters brief** command.

```
user@host> show ddos-protection protocols pppoe parameters brief
```

```
Number of policers modified: 1
Protocol  Packet      Bandwidth  Burst  Priority  Recover  Policer  Bypass  FPC
group     type        (pps)      (pkts)             time(sec) enabled aggr.  mod
pppoe     aggregate   800*       2000   medium    300      yes     --     no
pppoe     padi        500        500    low       300      yes     no     no
pppoe     pado        0          0      low       300      yes     no     no
pppoe     padr        500        500    medium    300      yes     no     no
pppoe     pads        0          0      low       300      yes     no     no
pppoe     padt        1000       1000   high      300      yes     no     no
pppoe     padm        0          0      low       300      yes     no     no
pppoe     padn        0          0      low       300      yes     no     no
```

From operational mode, enter the **show ddos-protection protocols pppoe padi** command, and enter the command for **padr** as well.

```
user@host> show ddos-protection protocols pppoe padi
```

```
Protocol Group: PPPoE

Packet type: padi (PPPoE PADI)
Individual policer configuration:
  Bandwidth:      500 pps
  Burst:          500 packets
  Priority:        low
  Recover time:   300 seconds
  Enabled:        Yes
  Bypass aggregate: No
System-wide information:
  Bandwidth for this packet type is being violated!
  Number of slots currently receiving excess traffic: 1
  Number of slots that have received excess traffic: 1
  Violation first detected at: 2011-03-09 11:26:33 PST
  Violation last seen at:    2011-03-10 12:03:44 PST
  Duration of violation: 1d 00:37 Number of violations: 1
  Received: 704832908          Arrival rate: 8000 pps
  Dropped: 660788548          Max arrival rate: 8008 pps
Routing Engine information:
```

```

Bandwidth: 500 pps, Burst: 500 packets, enabled
Policer is never violated
Received: 39950330      Arrival rate: 298 pps
Dropped: 0             Max arrival rate: 503 pps
Dropped by aggregate policer: 0
FPC slot 3 information:
Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
Policer is currently being violated!
Violation first detected at: 2011-03-09 11:26:35 PST
Violation last seen at: 2011-03-10 12:03:44 PST
Duration of violation: 1d 00:37 Number of violations: 1
Received: 704832908      Arrival rate: 8000 pps
Dropped: 664882578      Max arrival rate: 8008 pps
Dropped by this policer: 660788548
Dropped by aggregate policer: 4094030

```

```
user@host> show ddos-protection protocols pppoe padr
```

```
Protocol Group: PPPoE
```

```

Packet type: padr (PPPoE PADR)
Individual policer configuration:
Bandwidth: 500 pps
Burst: 500 packets
Priority: medium
Recover time: 300 seconds
Enabled: Yes
Bypass aggregate: No
System-wide information:
Bandwidth for this packet type is being violated!
Number of slots currently receiving excess traffic: 1
Number of slots that have received excess traffic: 1
Violation first detected at: 2011-03-10 06:21:17 PST
Violation last seen at: 2011-03-10 12:04:14 PST
Duration of violation: 05:42:57 Number of violations: 1
Received: 494663595      Arrival rate: 24038 pps
Dropped: 484375900      Max arrival rate: 24062 pps
Routing Engine information:
Bandwidth: 500 pps, Burst: 500 packets, enabled
Policer is never violated
Received: 10287695      Arrival rate: 500 pps
Dropped: 0             Max arrival rate: 502 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
Policer is currently being violated!
Violation first detected at: 2011-03-10 06:21:18 PST
Violation last seen at: 2011-03-10 12:04:14 PST
Duration of violation: 05:42:56 Number of violations: 1
Received: 494663595      Arrival rate: 24038 pps
Dropped: 484375900      Max arrival rate: 24062 pps
Dropped by this policer: 484375900
Dropped by aggregate policer: 0

```

Meaning The output from the `show ddos-protection protocols pppoe parameters brief` command lists the current configuration for each of the individual PPPoE packet policers and the PPPoE aggregate policer. A change from a default value is indicated by an asterisk next

to the modified value. The only change made to PPPoE policers in the configuration steps was to the aggregate policer bandwidth; this change is confirmed in the output. Besides the configuration values, the command output also reports whether a policer has been disabled, whether it bypasses the aggregate policer (meaning that the traffic for that packet type is not included for evaluation by the aggregate policer), and whether the policer has been modified for one or more line cards.

The output of the **show ddos-protection protocols pppoe padi** command in this example shows the following information:

- The **System-wide information** section shows that 704,832,908 PPPoE PADI packets were received across all line cards and the Routing Engine. The section shows a single violation on a line card that is still in progress, and that the aggregate policer at the line card dropped 660,788,548 of the PADI packets.
- The **FPC slot 3 information** section shows that this line card received all 704,832,908 PADI packets. Its individual policer dropped 660,788,548 of those packets and its aggregate policer dropped the other 4,094,030 packets. The violation is ongoing and has lasted more than a day.
- The **Routing Engine information** section shows that only 39,950,330 PADI packets reached the Routing Engine and that it dropped no additional packets.

The difference between the number of PADI packets received and dropped at the line card $[704,832,908 - (660,788,548 + 4,094,030)]$ matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 3 received any PADI packets.

The output of the **show ddos-protection protocols pppoe padr** command in this example shows the following information:

- The **System-wide information** section shows that 494,663,595 PPPoE PADR packets were received across all line cards and the Routing Engine. The section shows a single violation on a line card that is still in progress, and that the policer at the line card dropped 484,375,900 of the PADR packets.
- The **FPC slot 1 information** section shows that this line card received all 494,663,595 PADR packets. Its individual policer dropped 484,375,900 of those packets. The violation is ongoing and has lasted more than five hours.
- The **Routing Engine information** section shows that only 10,287,695 PADR packets reached the Routing Engine and that it dropped no additional packets.

The difference between the number of PADR packets received and dropped at the line card $(494,663,595 - 484,375,900)$ matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1 received any PADR packets.



NOTE: This scenario is unrealistic in showing all PADI packets received on one line card and all PADR packets on a different line card. The intent of the scenario is to illustrate how policer violations are reported for individual line cards.

**Related
Documentation**

- [Distributed Denial-of-Service \(DDoS\) Protection Overview on page 527](#)
- [Configuring DDoS Protection on page 535](#)

Example: Configuring DDoS Protection on QFX Series Switches

This example shows how to configure DDoS protection so a switch can quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources.

- [Requirements on page 556](#)
- [Overview on page 556](#)
- [Configuration on page 557](#)
- [Verification on page 559](#)

Requirements

DDoS protection requires the following hardware and software:

- QFX Series switch that supports DDoS protection
- Junos OS Release 15.1X53-D10 or later

No special configuration beyond device initialization is required before you can configure this feature.

Overview

Distributed denial-of-service (DDoS) attacks use multiple sources to flood a network with protocol control packets. This malicious traffic triggers a large number of exceptions in the network and attempts to exhaust the system resources to deny valid users access to the network or server.

DDoS protection is enabled by default on a supported QFX Series switch. This example describes how you can modify the default configuration for the rate-limiting policers that identify excess control traffic and drop the packets before the switch is adversely affected. Sample tasks include configuring an aggregate policer for a protocol group, configuring policers for particular control packet types within a protocol group, and specifying trace options for DDoS operations.

This example show how to change some of the default policer parameters and behavior for the **radius** protocol group and the Radius **accounting** packet type. You can use the

same commands to change policer limits for other supported protocol groups and packet types. See the [ddos-protection](#) configuration statement at the **[edit system]** hierarchy level for all available configuration options.

Configuration

CLI Quick Configuration To quickly configure DDoS protection for protocol groups and particular control packet types, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
[edit]
edit system
set ddos-protection protocols radius aggregate bandwidth 150
set ddos-protection protocols radius aggregate burst 2000
set ddos-protection protocols radius accounting bandwidth 100 burst 150
set ddos-protection protocols radius accounting priority low
set ddos-protection protocols radius server bypass-aggregate
set ddos-protection traceoptions file ddos-trace size 10m
set ddos-protection traceoptions flag all
top
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure DDoS protection:

1. Specify a protocol group.

```
[edit system ddos-protection protocols]
user@host# edit radius
```

2. Configure the maximum traffic rate for the RADIUS aggregate policer; that is, for the combination of all RADIUS packets.

```
[edit system ddos-protection protocols radius]
user@host# set aggregate bandwidth 150
```

3. Configure the maximum burst rate for the RADIUS aggregate policer.

```
[edit system ddos-protection protocols radius]
user@host# set aggregate burst 2000
```

4. Configure a different maximum traffic rate and burst size for RADIUS accounting packets.

```
[edit system ddos-protection protocols radius]
```

```
user@host# set accounting bandwidth 100 burst 1500
```

5. Decrease the priority for RADIUS accounting packets.

```
[edit system ddos-protection protocols radius]
user@host# set accounting priority low
```

6. Prevent RADIUS server control packets from being included in the aggregate bandwidth; that is, server packets do not contribute toward the combined RADIUS traffic to determine whether the aggregate bandwidth is exceeded. However, the server packets are still included in traffic rate statistics.

```
[edit system ddos-protection protocol radius]
user@host# set server bypass-aggregate
```

7. (On switches with multiple line cards only) Reduce the bandwidth and burst size allowed before a violation is declared for the RADIUS policer on the FPC in slot 1.

```
[edit system ddos-protection protocols radius]
user@host# set aggregate fpc 1 bandwidth-scale 80
user@host# set aggregate fpc 1 burst-scale 75
```

8. Configure tracing for all DDoS protocol processing events.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos-log
user@host# set file size 10m
user@host# set flag all
```

Results From configuration mode, confirm your configuration by entering the **show ddos-protection** command at the **system** hierarchy level.

```
[edit system]
user@host# show ddos-protection

traceoptions {
  file ddos-log size 10m;
  flag all;
}
protocols {
  radius {
    aggregate {
      bandwidth 150;
      burst 2000;
    }
    server {
```

```

        bypass-aggregate;
    }
    accounting {
        bandwidth 100;
        burst 1500;
        priority low;
    }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the DDoS protection configuration is working properly, perform these tasks:

- [Verifying the DDoS Protection Configuration on page 559](#)

Verifying the DDoS Protection Configuration

Purpose Verify that the RADIUS policer values have changed from the default.

Action From operational mode, enter the **show ddos-protection protocols radius parameters** command.

```

user@host> show ddos-protection protocols radius parameters
Packet types: 5, Modified: 3
* = User configured value

Protocol Group: Radius

Packet type: aggregate (Aggregate for all Radius traffic)
Aggregate policer configuration:
  Bandwidth:      150 pps*
  Burst:          2000 packets*
  Recover time:   300 seconds
  Enabled:        Yes
Routing Engine information:
  Bandwidth: 150 pps, Burst: 2000 packets, enabled
FPC slot 0 information:
  Bandwidth: 100% (150 pps), Burst: 100% (2000 packets), enabled

Packet type: server (Radius server traffic)
Individual policer configuration:
  Bandwidth:      200 pps
  Burst:          2048 packets
  Priority:        High
  Recover time:   300 seconds
  Enabled:        Yes
  Bypass aggregate: Yes*
Routing Engine information:
  Bandwidth: 200 pps, Burst: 2048 packets, enabled
FPC slot 0 information:

```

```
Bandwidth: 100% (200 pps), Burst: 100% (2048 packets), enabled

Packet type: accounting (Radius accounting traffic)
Individual policer configuration:
  Bandwidth:      100 pps*
  Burst:          1500 packets*
  Priority:        Low*
  Recover time:    300 seconds
  Enabled:         Yes
  Bypass aggregate: No
Routing Engine information:
  Bandwidth: 100 pps, Burst: 1500 packets, enabled
FPC slot 0 information:
  Bandwidth: 100% (100 pps), Burst: 100% (1500 packets), enabled

Packet type: authorization (Radius authorization traffic)
Individual policer configuration:
  Bandwidth:      200 pps
  Burst:          2048 packets
  Priority:        High
  Recover time:    300 seconds
  Enabled:         Yes
  Bypass aggregate: No
Routing Engine information:
  Bandwidth: 200 pps, Burst: 2048 packets, enabled
FPC slot 0 information:
  Bandwidth: 100% (200 pps), Burst: 100% (2048 packets), enabled
```

Meaning The command output shows the current configuration of the RADIUS aggregate policer and the RADIUS accounting, server, and authorization control packet policers. Policer values that have been modified from the default values are marked with an asterisk. The output shows that the RADIUS policer configuration has been modified correctly.

Related Documentation

- [Distributed Denial-of-Service \(DDoS\) Protection Overview on page 527](#)
- [Configuring DDoS Protection on page 535](#)

Rate Limiting ICMPv4 and ICMPv6 Traffic

To limit the rate at which ICMPv4 or ICMPv6 messages can be generated by the Routing Engine and sent to the Routing Engine, include the appropriate rate limiting statement at the `[edit system internet-options]` hierarchy level:

- For IPv4:
 - `icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate`
- For IPv6:

- icmpv6-rate-limit bucket-size *bucket-size* packet-rate *packet-rate*

The bucket size is the number of seconds in the rate-limiting bucket. The packet rate is the rate-limiting packets earned per second. Specify a **bucket-size** from 0 through 4294967295 seconds. The default value is 5 seconds. Specify a **packet-rate** from 0 through 4,294,967,295. The default value is 1000.

Related • *internet-options*
Documentation

PART 10

Flow Detection

- [Flow Detection and Culprit Flows on page 565](#)

CHAPTER 23

Flow Detection and Culprit Flows

- [DDoS Protection Flow Detection Overview on page 565](#)
- [Setting Up and Using Flow Detection on page 568](#)
- [Configuring How Flow Detection Operates Globally on page 576](#)
- [Configuring How Traffic in a Culprit Flow Is Controlled Globally on page 578](#)

DDoS Protection Flow Detection Overview

Flow detection is an enhancement to DDoS protection that supplements the DDoS policer hierarchies; it is part of a complete DDoS protection solution. Flow detection uses a limited amount of hardware resources to monitor the arrival rate of host-bound flows of control traffic. Flow detection is much more scalable than a solution based on filter policers. Filter policers track all flows, which consumes a considerable amount of resources. In contrast, flow detection only tracks flows it identifies as suspicious, using far fewer resources to do so.

The flow detection application has two interrelated components, detection and tracking. Detection is the process where flows suspected of being improper are identified and subsequently controlled. Tracking is the process where flows are tracked to determine whether they are truly hostile and when these flows recover to within acceptable limits.

- [Flow Detection and Control on page 565](#)
- [Flow Tracking on page 566](#)
- [Notifications on page 567](#)

Flow Detection and Control

Flow detection is disabled by default. When you enable it at the **[edit system ddos-protection global]** hierarchy level, the application begins monitoring control traffic flows when a DDoS protection policer is violated for almost all protocol groups and packet types. In addition to enabling flow detection globally, you can configure its operation mode—that is, whether it is automatically triggered by the violation of a DDoS protection policer (the default) or is always on—for almost all protocol groups and packet types. You can override the global configuration settings for individual protocol groups and packet types. Other than event report rates, all other characteristics of flow detection are configurable only at the level of individual packet types.

Enhanced Subscriber Management supports flow detection for DDoS protection as of Junos OS Release 17.3R1.



NOTE: You cannot enable flow detection globally for the following groups and packet type because they do not have typical Ethernet, IP, or IPv6 headers:

- Protocol groups: **fab-probe**, **frame-relay**, **inline-ka**, **isis**, **jfm**, **mlp**, **pfe-alive**, **pos**, and **services**.
- Packet type: **unclassified** in the **ip-options** protocol group.

Control flows are aggregated at three levels. The *subscriber level* is the finest grained of the three and consists of flows for individual subscriber sessions. The *logical interface level* aggregates multiple subscriber flows, so it is coarser grained and does not provide discrimination into individual subscriber flows. The *physical interface level* aggregates multiple logical interface flows, so it provides the coarsest view of traffic flows.

You can turn flow detection off or on at any of these levels. You can also configure whether it is automatically triggered by the violation of a DDoS protection policer or is always on. Flow detection begins at the finest-grained level that has detection configured to **on** or **automatic**.

When a flow arrives, flow detection checks whether the flow is already listed in a table of *suspicious* flows. A suspicious flow is one that exceeds the bandwidth allowed by default or configuration. If the flow is not in the table and the aggregation level flow detection mode is **on**, then flow detection lists the flow in the table. If the flow is not in the table and the flow detection mode is **automatic**, flow detection checks whether this flow is suspicious.

If the flow is suspicious, then it goes in the flow table. If the flow is not suspicious, then it is processed the same way at the next coarser aggregation level that has flow detection set to **on**. If none of the higher levels have detection on, then the flow continues to the DDoS protection packet policer for action, where it can be passed or dropped.

When the initial check finds the flow in the table, then the flow is dropped, policed, or kept, depending on the control mode setting for that aggregation level. All packets in dropped flows are dropped. In policed flows, packets are dropped until the flow is within the acceptable bandwidth for the aggregation level. Kept flows are passed along to the next aggregation level for processing.

Flow Tracking

The flow detection application tracks flows that have been listed in the suspicious flow table. It periodically checks each entry in the table to determine whether the listed flow is still suspicious (violating the bandwidth). If a suspicious flow has continuously violated the bandwidth since it was inserted in the table for a period greater than the configurable flow detection period, then it is considered to be a *culprit* flow rather than merely suspicious. However, if the bandwidth has been violated for less than the detection period,

the violation is treated as a false positive. Flow detection considers the flow to be safe and stops tracking it (deletes it from the table).

You can enable a timeout feature that suppresses culprit flows for a configurable timeout period, during which the flow is kept in the flow table. (Suppression is the default behavior, but the flow detection action can be changed by the flow level control configuration.) If the check of listed flows finds one for which the timeout is enabled and the timeout period has expired, then the flow has timed out and it is removed from the flow table.

If the timeout has not yet expired or if the timeout feature is not enabled, then the application performs a recovery check. If the time since the flow last violated the bandwidth is longer than the configurable recovery period, the flow has recovered and is removed from the flow table. If the time since last violation is less than the recovery period, the flow is kept in the flow table.

Notifications

By default, flow detection automatically generates system logs for a variety of events that occur during flow detection. The logs are referred to as *reports* in the flow detection CLI. All protocol groups and packet types are covered by default, but you can disable automatic logging for individual packet types. You can also configure the rate at which reports are sent, but this applies globally to all packet types.

Each report belongs to one of the following two types:

- Flow reports—These reports are generated by events associated with the identification and tracking of culprit flows. Each report includes identifying information for the flow that experienced the event. This information is used to accurately maintain the flow table; flows are deleted or retained in the table based on the information in the report.

[Table 32 on page 567](#) describes the event that triggers each flow report.

Table 32: Triggering Event for Flow Detection Reports

Name	Description
DDOS_SCFD_FLOW_FOUND	A suspicious flow is detected.
DDOS_SCFD_FLOW_TIMEOUT	The timeout period expires for a culprit flow. Flow detection stops suppressing (or monitoring) the flow.
DDOS_SCFD_FLOW_RETURN_NORMAL	A culprit flow returns to within the bandwidth limit.
DDOS_SCFD_FLOW_CLEARED	A culprit flow is cleared manually with a clear command or automatically as the result of suspicious flow monitoring shifting to a different aggregation level.
DDOS_SCFD_FLOW_AGGREGATED	Control flows are aggregated to a coarser level. This event happens when the flow table nears capacity or when the flow cannot be found at a particular flow level and the next coarser level has to be searched.
DDOS_SCFD_FLOW_DEAGGREGATED	Control flows are deaggregated to a finer level. This event happens when the flow table is not very full or when flow control is effective and the total arrival rate for the flow at the policer for the packet type is below its bandwidth for a fixed, internal period.

- **Bandwidth violation reports**—These reports are generated by events associated with the discovery of suspicious flows. Each report includes identifying information for the flow that experienced the event. This information is used to track the suspicious flow and identify flows that are placed in the flow table. [Table 33 on page 568](#) describes the event that triggers each violation report.

Table 33: Triggering Event for Bandwidth Violation Reports

Name	Description
DDOS_PROTOCOL_VIOLATION_SET	The incoming traffic for a control protocol exceeded the configured bandwidth.
DDOS_PROTOCOL_VIOLATION_CLEAR	The incoming traffic for a violated control protocol returned to normal.

A report is sent only when triggered by an event; that is, there are no null or empty reports. Because the reports are made periodically, the only events of interest are ones that occur during the interval since the last report.

Release History Table

Release	Description
17.3R1	Enhanced Subscriber Management supports flow detection for DDoS protection as of Junos OS Release 17.3R1.

Related Documentation

- [Configuring Flow Detection for DDoS Protection](#)

Setting Up and Using Flow Detection

Flow detection monitors the flows of control traffic for violation of the bandwidth allowed for each flow and manages traffic identified as a culprit flow. Suppression of the traffic is the default management option. Flow detection is typically implemented as part of an overall DDoS protection strategy, but it is also useful for troubleshooting and understanding traffic flow in new configurations. Flow detection is disabled by default.

Enhanced Subscriber Management supports flow detection for DDoS protection as of Junos OS Release 17.3R1.

Before you begin, ensure you have configured DDoS protection appropriately for you network. See *OBSOLETE: Configuring Protection Against DDoS Attacks* for detailed information about DDoS protection.

- [Configuring the Detection Period for Suspicious Flows on page 569](#)
- [Configuring the Recovery Period for a Culprit Flow on page 569](#)
- [Configuring the Timeout Period for a Culprit Flow on page 570](#)
- [Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 571](#)
- [Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 572](#)

- [Enabling Flow Detection for All Protocol Groups and Packet Types on page 573](#)
- [Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types on page 574](#)
- [Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types on page 574](#)
- [Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 574](#)
- [Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 575](#)
- [Verifying and Managing Flow Detection on page 575](#)

Configuring the Detection Period for Suspicious Flows

DDoS protection flow detection considers a monitored flow to be a suspicious flow whenever the flow exceeds its allowed bandwidth, based on a crude test that eliminates obviously good flows from consideration. A closer examination of a suspicious flow requires the flow to remain in violation of the bandwidth for a period of time before flow detection considers it to be a culprit flow against which it must take action. You can include the **flow-detect-time** statement to configure the duration of this detection period or you can rely on the default period of three seconds.

Enhanced Subscriber Management supports flow detection for DDoS protection as of Junos OS Release 17.3R1.



BEST PRACTICE: We recommend that you use the default value for the detection period.

To specify how long a flow must be in violation before flow detection declares it to be a culprit flow:

- Set the detection period.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set flow-detect-time seconds
```

For example, include the following statement to require the DHCPv4 discover packet flow to be in violation of its allowed bandwidth for 30 seconds before it is considered to be a culprit flow:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set flow-detect-time 30
```

Configuring the Recovery Period for a Culprit Flow

After DDoS protection flow detection has identified a suspicious flow as a culprit flow, it has to determine when that flow no longer represents a threat to the router. When the traffic flow rate drops back to within the allowed bandwidth, the rate must remain within the bandwidth for a recovery period. Only then does flow detection consider the flow to be normal and stop the traffic handling action enacted against the culprit flow. You can

include the **flow-recover-time** statement to configure the duration of this recovery period or you can rely on the default period of 60 seconds.

To specify how long a flow must be within its allowed bandwidth after a violation before flow detection declares it to be a normal flow:

- Set the recovery period.

```
[edit system ddos-protection protocols protocol-group packet-type]  
user@host# set flow-recover-time seconds
```

For example, include the following statement to require the DHCPv4 discover packet flow to be in recovery for five minutes (300 seconds):

```
[edit system ddos-protection protocols dhcpv4 discover]  
user@host# set flow-recover-time 300
```

Configuring the Timeout Period for a Culprit Flow

When DDoS protection flow detection identifies a suspicious flow as a culprit flow, by default it suppresses traffic for that flow for as long as the traffic flow exceeds the bandwidth limit. Suppression stops and the flow is removed from the flow table when the time since the last violation by the flow is greater than the recovery period.

Alternatively, you can include the **timeout-active-flows** statement to enable flow detection to suppress a culprit flow for a configurable timeout period. When the timeout period expires, suppression stops and the flow is removed from the flow table. You can either include the **flow-timeout-time** statement to configure the duration of the timeout period or rely on the default timeout of 300 seconds.

To enable flow detection to suppress a culprit flow for a timeout period:

1. Enable the timeout.

```
[edit system ddos-protection protocols protocol-group packet-type]  
user@host# set timeout-active-flows
```

2. Specify the timeout period.

```
[edit system ddos-protection protocols protocol-group packet-type]  
user@host# set flow-timeout-time seconds
```

For example, include the following statements to suppress the DHCPv4 discover packet flow for 10 minutes (600 seconds):

```
[edit system ddos-protection protocols dhcpv4 discover]  
user@host# set timeout-active-flows  
user@host# set flow-timeout-time 600
```

Configuring How Flow Detection Operates at Each Flow Aggregation Level

When flow detection is turned on, traffic flows are monitored by default for all protocol groups and packet types. When a policer violation occurs, each suspicious flow is examined to determine whether it is the culprit flow that caused the violation. You can include the **flow-level-detection** statement to configure how flow detection works at each flow aggregation level for a packet type: subscriber, logical interface, or physical interface.



NOTE: The flow detection mode at the packet level must be either **automatic** or **on** for flow detection to operate at individual flow aggregation levels.

Like flow detection at the protocol group and packet level, flow detection at the flow aggregation level supports three modes:

- **automatic**—When a DDoS protection policer is violated, traffic flows at this flow aggregation level are monitored for suspicious behavior only until flow detection determines that the suspect flow is not at this aggregation level and instead must be at a coarser level of aggregation. Flows at this level are subsequently not searched again until the policer is no longer violated at the coarser level.
- **off**—Traffic flows are never monitored at this flow aggregation level.
- **on**—Traffic flows at this flow aggregation level are monitored for suspicious flows even when no DDoS protection policer is currently being violated, if flow detection at the packet level is configured to **on**. Monitoring continues at this level regardless of whether a suspect flow is identified at this level. However, if the packet level mode is **automatic**, then the policer must be in violation for traffic flows to be checked at this level.

Flows are examined first at the finest-grained (lowest bandwidth) flow aggregation level, subscriber. If the suspect flow is not found at the subscriber level, then flows are checked at the logical interface level. Finally, if the suspect is not found there, then flows are checked at the physical interface level; barring some misconfiguration, the culprit flow must be found at this level.

To configure how flow detection operates at each flow aggregation level:

1. (Optional) Specify the detection mode at the subscriber level.

```
[edit system ddos-protection protocols protocol-group packet-type flow-level-detection]
user@host# set subscriber flow-detection-mode
```

2. (Optional) Specify the detection mode at the logical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type flow-level-detection]
user@host# set logical-interface flow-detection-mode
```

3. (Optional) Specify the detection mode at the physical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type flow-level-detection]
user@host# set physical-interface flow-detection-mode
```

For example, include the following statements to configure flow detection to check for suspicious flows at the subscriber level only when the policer is being violated, to never check at the logical interface level, and to always check at the physical interface level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-detection
user@host# set subscriber automatic
user@host# set logical-interface off
user@host# set physical-interface on
```

Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level

When flow detection is enabled, all traffic in a culprit flow is dropped by default for all protocol groups and packet types and at all flow aggregation levels. You can include the **flow-level-control** statement to configure flow detection to control traffic differently for individual packet types. You have to specify the control behavior at a particular flow aggregation level: subscriber, logical interface, or physical interface.

You can configure flow detection flow control to employ one of the following modes for a packet type:

- Drop all traffic—Configure flow control to drop all traffic when you think the flow that is violating a bandwidth limit is malicious. This behavior is the default at all flow aggregation levels.
- Police traffic—Configure flow control to police a flow that is violating bandwidth, forcing the rate below the bandwidth limit. Flow control acts as a simple policer in this case.
- Keep all traffic—Configure flow control to keep all traffic whether the flow is in violation or below the bandwidth limit. This mode is helpful when you need to debug traffic flow for your network.

Flow control mode enables great flexibility in how you manage control traffic in your network. For example, if you only want to ensure that control flows for a packet type at all aggregation levels are within their limits, you can configure flow control to police the traffic at each level. Or if you want to detect culprit flows and suppress them at one level but only restrain traffic to the allowed bandwidth at another level, you can configure one level to drop all traffic and the other to police traffic.

To configure how flow detection controls traffic in a culprit flow:

1. (Optional) Specify the control mode at the subscriber level.

```
[edit system ddos-protection protocols protocol-group packet-type flow-level-control]
user@host# set subscriber flow-control-mode
```

2. (Optional) Specify the control mode at the logical interface level.


```
[edit system ddos-protection protocols protocol-group packet-type flow-level-control]
user@host# set logical-interface flow-control-mode
```

3. (Optional) Specify the control mode at the physical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type flow-level-control]
user@host# set physical-interface flow-control-mode
```

For example, to configure flow detection to keep all traffic for a physical interface under the configured bandwidth, but detect and suppress culprit flows at the subscriber level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-control
user@host# set subscriber drop
user@host# set physical-interface police
user@host# edit flow-level-detection
user@host# set logical-interface off
```

In this example, you do not care about the logical interface, so flow detection is turned off for that level. Because flow detection is disabled, the state of flow control for that level does not matter.

Enabling Flow Detection for All Protocol Groups and Packet Types

By default, flow detection is disabled for all protocol groups and packet types. You must enable flow detection globally by including the **flow-detection** statement. If you subsequently disable flow detection for individual packet types, you cannot use this global statement to override all such individual configurations; you must re-enable detection at the packet configuration level.

To enable flow detection globally:

- Set flow detection.

```
[edit system ddos-protection global]
user@host# set flow-detection
```



NOTE: You cannot enable flow detection globally for the following groups and packet type because they do not have typical Ethernet, IP, or IPv6 headers:

- Protocol groups: fab-probe, frame-relay, inline-ka, isis, jfm, mlp, pfe-alive, pos, and services.
- Packet type: unclassified in the ip-options protocol group.

Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types

When flow detection confirms that a suspicious flow it is tracking on a line card is indeed a culprit flow, it sends a report to the Routing Engine. Flow detection also reports each culprit flow that subsequently recovers to within the allowed bandwidth or is cleared. You can include the **flow-report-rate** statement to limit how many flows per second on each line card can be reported. Culprit flow events are reported for all protocol groups and packet types by default. When too many flows are reported, congestion can occur on the host path to the Routing Engine flow.

To globally configure the maximum report rate for culprit flows:

- Set the reporting rate.

```
[edit system ddos-protection global]  
user@host# set flow-report-rate rate
```

Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types

By default, flow detection reports to the Routing Engine all violations of bandwidth at the FPC for all protocol groups and packet types. You can include the **violation-report-rate** statement to limit how many violations per second flow detection reports from the line cards, thus reducing the load on the router. We recommend that you configure a report rate that is suitable for your network rather than rely on the default value.

To globally configure the maximum bandwidth violation reporting rate:

- Set the reporting rate.

```
[edit system ddos-protection global]  
user@host# set violation-report-rate rate
```

Disabling Automatic Logging of Culprit Flow Events for a Packet Type

By default, flow detection automatically logs policer violation events associated with suspicious flows (violation reports) and culprit flow events (flow reports) for all protocol groups and packet types. You can include the **no-flow-logging** statement to prevent automatic logging of culprit flow events for individual packet types. Automatic logging of suspicious flow violation events is disabled with the **disable-logging** statement at the **[edit system ddos-protection global]** hierarchy level.

To disable automatic culprit flow event logging for a packet type:

- Disable logging.

```
[edit system ddos-protection protocols protocol-group packet-type]  
user@host# set no-flow-logging
```

To disable automatic suspicious flow violation event logging for a packet type:

- Disable logging.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set disable-logging
```

For example, include the following statement to disable automatic logging for DHCPv4 DISCOVER packet flows:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set no-flow-logging
```

Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level

You can include the **flow-level-bandwidth** statement to configure the maximum acceptable bandwidth for traffic flows for individual packet types. You have to specify the bandwidth behavior at a particular flow aggregation level: subscriber, logical interface, or physical interface. We recommend that you tune the bandwidth values for your network rather than rely on the defaults.

To configure the maximum bandwidth for traffic flows each flow aggregation level:

1. (Optional) Configure the bandwidth for flows at the subscriber level.

```
[edit system ddos-protection protocols protocol-group packet-type
flow-level-bandwidth]
user@host# set subscriber flow-bandwidth
```

2. (Optional) Configure the bandwidth for flows at the logical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type
flow-level-bandwidth]
user@host# set logical-interface flow-bandwidth
```

3. (Optional) Configure the bandwidth for flows at the physical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type
flow-level-bandwidth]
user@host# set physical-interface flow-bandwidth
```

For example, to configure the flow bandwidth to 1000 pps at the subscriber level, 5000 pps at the logical interface level, and 30,000 at the physical interface level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-bandwidth
user@host# set subscriber 1000
user@host# set logical-interface 5000
user@host# set physical-interface 30000
```

Verifying and Managing Flow Detection

Purpose View or clear information about flow detection as part of a DDoS protection configuration.

Enhanced Subscriber Management supports flow detection for DDoS protection as of Junos OS Release 17.3R1.

- Action**
- To display configuration information for flow detection:

```
user@host> show ddos-protection protocols flow-detection
```

- To display information about culprit flows identified by flow detection, including number of flows detected and tracked, source address of the flow, arriving interface, and rates:

```
user@host> show ddos-protection protocols culprit-flows
```

- To clear culprit flows for all packet types in all protocol groups:

```
user@host> clear ddos-protection protocols culprit-flows
```

- To clear culprit flows for all packet types in a particular protocol group:

```
user@host> clear ddos-protection protocols protocol-group culprit-flows
```

Release History Table

Release	Description
17.3R1	Enhanced Subscriber Management supports flow detection for DDoS protection as of Junos OS Release 17.3R1.
17.3R1	Enhanced Subscriber Management supports flow detection for DDoS protection as of Junos OS Release 17.3R1.
17.3R1	Enhanced Subscriber Management supports flow detection for DDoS protection as of Junos OS Release 17.3R1.

- Related Documentation**
- Configuring Flow Detection for DDoS Protection*

Configuring How Flow Detection Operates Globally

Flow detection is disabled globally for all protocol groups and packet types by default. After you have turned on flow detection globally with the `flow-detection` statement at the `[edit system ddos-protection global]` hierarchy level, you can include the `flow-detection-mode` statement to configure *how* flow detection operates globally for all protocol groups and packet types. By default, flow detection operates in automatic mode for all packet types, meaning that it monitors control traffic for suspicious flows only after a DDoS policer has been violated. You can also configure flow detection either to never monitor flows or to always monitor flows.

When flow detection is turned on, traffic flows are monitored by default for all protocol groups and packet types. You can override the global configuration by including the `flow-detection-mode` statement at the `[edit system ddos-protection protocols`

protocol-group packet-type] hierarchy level to configure how flow detection works for a protocol group or a packet type. You can also use the **flow-level-detection** statement to specify the behavior for one or more traffic flow aggregation levels (subscriber, logical interface, or physical interface).



CAUTION: In a virtual chassis configuration, we recommend that you override flow detection for all Virtual Chassis control packets. The flow is based on the MAC address of the module in the FPC slot. If the virtual-chassis control-low flow is in violation, then all control traffic is lost, resulting in unexpected behavior. This behavior can include DHCP and PPPoE control traffic loss, loss of ARP requests, routing protocol flaps, and more.

To override flow detection for Virtual Chassis control packets when you have enabled global flow detection:

- Disable flow detection for each packet type.

```
[edit]
user@host# set system ddos-protection protocols virtual-chassis control-low
flow-detection-mode off
user@host# set system ddos-protection protocols virtual-chassis
control-high flow-detection-mode off
user@host# set system ddos-protection protocols virtual-chassis
unclassified flow-detection-mode off
user@host# set system ddos-protection protocols virtual-chassis vc-packets
flow-detection-mode off
user@host# set system ddos-protection protocols virtual-chassis
vc-ttl-errors flow-detection-mode off
```

Flow detection supports the following three modes:

- **automatic**—When a DDoS protection policer is violated, traffic flows where the violation occurred are monitored for suspicious behavior. Each suspicious flow is examined to determine whether it is the culprit flow that caused the violation.
- **off**—Traffic flows are never monitored for any protocol group or packet type.
- **on**—Traffic flows for all protocol groups and packet types are monitored for suspicious flows even when no DDoS protection policer is currently being violated.



NOTE: The detection mode is set to automatic by default. This means that if you enable global flow-detection and do not specify a mode, then flows are detected only when the policer is being violated.

To configure how flow detection operates at each flow aggregation level:

- Specify the detection mode.

```
[edit system ddos-protection protocols global]
```

```
user@host# set flow-detection-mode flow-detection-mode
```

For example, to configure flow detection to always monitor and detect flows for all protocol groups and packet types at all flow aggregation levels:

```
[edit system ddos-protection global]  
user@host# set flow-detection-mode on
```

Configuring How Traffic in a Culprit Flow Is Controlled Globally

When flow detection is enabled, all traffic in a culprit flow is dropped by default for all protocol groups and packet types and at all flow aggregation levels. You can include the **flow-level-control** statement to configure how flow detection controls traffic for all traffic flow aggregation levels globally for all protocol groups and packet types. You cannot specify the control behavior globally for a particular flow aggregation level: subscriber, logical interface, or physical interface. To do that, you must override the global configuration with the **flow-level-control** statement at the **[edit system ddos-protection protocols protocol-group packet-type]** hierarchy level.

You can configure flow detection flow control to employ one of the following modes:

- Drop all traffic—Configure flow control to drop all traffic when you think the flow that is violating a bandwidth limit is malicious. This behavior is the default at all flow aggregation levels for all protocol groups and packet types.
- Police traffic—Configure flow control to police a flow that is violating bandwidth, forcing the rate below the bandwidth limit. Flow control acts as a simple policer in this case.
- Keep all traffic—Configure flow control to keep all traffic whether the flow is in violation or below the bandwidth limit. This mode is helpful when you need to debug traffic flow for your network.

To configure how flow detection controls traffic in a culprit flow for all flow aggregation levels for all protocol groups and packet types:

- Specify the control mode.

```
[edit system ddos-protection global]  
user@host# set flow-level-control flow-control-mode
```

Flow control mode enables great flexibility in how you manage control traffic in your network. For example, if you only want to ensure that control flows for all packet types at all aggregation levels are within their limits, you can configure flow control globally to police the traffic.

```
[edit system ddos-protection global]  
user@host# set flow-level-control police
```

Or, suppose you want to detect culprit flows and suppress them for DHCP discover packets at the physical interface flow aggregation level, but only restrain all traffic to the

allowed bandwidth at the other levels. You can configure the police action globally, then override it for the packet type and physical level by configuring that level to drop all traffic.

```
[edit system ddos-protection global]  
user@host# set flow-level-control police  
[edit system ddos-protection protocols dhcpv4 discover ]  
user@host# set flow-level-control physical-interface drop
```


PART 11

Unicast Forwarding

- [Unicast Reverse Path Forwarding on page 583](#)
- [Unknown Unicast Forwarding on page 613](#)

CHAPTER 24

Unicast Reverse Path Forwarding

- [Understanding Unicast RPF \(Switches\) on page 584](#)
- [Understanding Unicast RPF \(Routers\) on page 588](#)
- [Example: Configuring Unicast RPF \(On a Switch\) on page 598](#)
- [Example: Configuring Unicast RPF \(On a Router\) on page 603](#)

Understanding Unicast RPF (Switches)

To protect against IP spoofing, and some types of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, unicast reverse-path-forwarding (RPF) verifies that packets are arriving from a legitimate path. It does this by checking the source address of each packet that arrives on an untrusted ingress interface and, comparing it to the forwarding-table entry for its source address. If the packet is from a valid path, that is, one that the sender would use to reach the destination, the device forwards the packet to the destination address. If it is not from a valid path, the device discards the packet. Unless it is protected against, IP spoofing can be an effective way for intruders to pass IP packets to a destination as genuine traffic, when in fact the packets are not actually meant for the destination.

Unicast RPF is supported for the IPv4 and IPv6 protocol families, as well as for the virtual private network (VPN) address family. Unicast RPF is not supported on interfaces configured as tunnel sources. This affects only the transit packets exiting the tunnel.

There are two modes of unicast RPF, *strict mode*, and *loose mode*. The default is strict mode, which means the switch forwards a packet only if the receiving interface is the best return path to the packet's unicast source address. Strict mode is especially useful on untrusted interfaces (where untrusted users or processes can place packets on the network segment), and for symmetrically routed interfaces (see [“When to Enable Unicast RPF” on page 586.](#)) For more information about strict unicast RPF, see RFC 3704, *Ingress Filtering for Multihomed Networks* at <http://www.ietf.org/rfc/rfc3704.txt>.

To enable strict mode unicast RPF on a selected customer-edge interface:

[edit interfaces]

```
user@switch# set interface-name unit 0 family inet rpf-check
```

The other mode is loose mode, which means the system checks to see if the packet has a source address with a corresponding prefix in the routing table, but it does not check whether the receiving interface is the best return path to the packet's unicast source address.

To enable unicast RPF loose mode, enter:

[edit interfaces]

```
user@switch# set interface-name unit 0 family inet rpf-check mode loose
```



NOTE: On Juniper Networks EX3200, EX4200, and EX4300 Ethernet Switches, the switch applies unicast RPF *globally* to all interfaces when unicast RPF is configured on any interface. For additional information, see [“Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches” on page 588.](#)

- [Unicast RPF for Switches Overview on page 585](#)
- [Unicast RPF Implementation on page 585](#)
- [When to Enable Unicast RPF on page 586](#)
- [When Not to Enable Unicast RPF on page 587](#)
- [Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches on page 588](#)

Unicast RPF for Switches Overview

Unicast RPF functions as an ingress filter that reduces the forwarding of IP packets that might be spoofing an address. By default, unicast RPF is disabled on the switch interfaces. The switch supports only the active paths method of determining the best return path back to a unicast source address. The active paths method looks up the best reverse path entry in the forwarding table. It does not consider alternate routes specified using routing-protocol-specific methods when determining the best return path.

If the forwarding table lists the receiving interface as the interface to use to forward the packet back to its unicast source, it is the best return path interface.

Unicast RPF Implementation

- [Unicast RPF Packet Filtering on page 585](#)
- [Bootstrap Protocol \(BOOTP\) and DHCP Requests on page 585](#)
- [Default Route Handling on page 585](#)

Unicast RPF Packet Filtering

When you enable unicast RPF on the switch, the switch handles traffic in the following manner:

- If the switch receives a packet on the interface that is the best return path to the unicast source address of that packet, the switch forwards the packet.
- If the best return path from the switch to the packet's unicast source address is not the receiving interface, the switch discards the packet.
- If the switch receives a packet that has a source IP address that does not have a routing entry in the forwarding table, the switch discards the packet.

Bootstrap Protocol (BOOTP) and DHCP Requests

Bootstrap protocol (BOOTP) and DHCP request packets are sent with a broadcast MAC address and therefore the switch does not perform unicast RPF checks on them. The switch forwards all BOOTP packets and DHCP request packets without performing unicast RPF checks.

Default Route Handling

If the best return path to the source is the default route (0.0.0.0) and the default route points to **reject**, the switch discards the packets. If the default route points to a valid network interface, the switch performs a normal unicast RPF check on the packets.



NOTE: On the EX4300, the default route is not used when the switch is configured in unicast RPF strict mode.

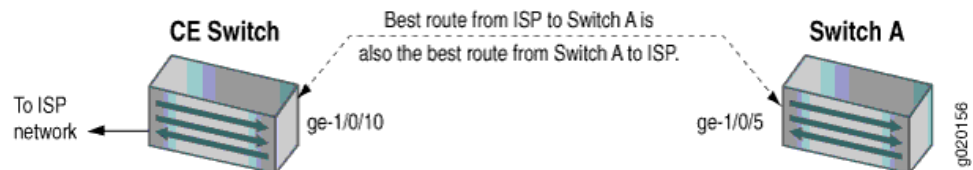
When to Enable Unicast RPF

Enable unicast RPF when you want to ensure that traffic arriving on a network interface comes from a source that resides on a network that interface can reach. You can enable unicast RPF on untrusted interfaces to filter spoofed packets. For example, a common application for unicast RPF is to help defend an enterprise network from DoS/DDoS attacks coming from the Internet.

Enable unicast RPF only on symmetrically routed interfaces, and as close as possible to the traffic source stops spoofed traffic before it can proliferate or reach interfaces that do not have unicast RPF enabled. Because unicast RPF is enabled globally on EX3200, EX4200, and EX4300 switches, ensure that *all* interfaces are symmetrically routed before you enable unicast RPF on these switches, as shown in [Figure 39 on page 586](#). Enabling unicast RPF on asymmetrically routed interfaces results in packets from legitimate sources being filtered. A symmetrically routed interface uses the same route in both directions between the source and the destination.

Unicast RPF is enabled globally on EX3200, EX4200, and EX4300 switches, to with these devices, be sure that *all* interfaces are symmetrically routed before you enable unicast RPF on these switches. Enabling unicast RPF on asymmetrically routed interfaces results in packets from legitimate sources being filtered.

Figure 39: Symmetrically Routed Interfaces



The following switch interfaces are most likely to be symmetrically routed and thus are candidates for unicast RPF enabling:

- The service provider edge to a customer
- The customer edge to a service provider
- A single access point out of the network (usually on the network perimeter)
- A terminal network that has only one link

On EX3200, EX4200, and EX4300 switches, we recommend that you enable unicast RPF explicitly on either all interfaces or only one interface. To avoid possible confusion, do not enable it on only some interfaces:

- Enabling unicast RPF explicitly on only one interface makes it easier if you choose to disable it in the future because you must explicitly disable unicast RPF on every interface on which you explicitly enabled it. If you explicitly enable unicast RPF on two interfaces

and you disable it on only one interface, unicast RPF is still implicitly enabled globally on the switch. The drawback of this approach is that the switch displays the flag that indicates that unicast RPF is enabled only on interfaces on which unicast RPF is explicitly enabled, so even though unicast RPF is enabled on all interfaces, this status is not displayed.

- Enabling unicast RPF explicitly on all interfaces makes it easier to know whether unicast RPF is enabled on the switch because every interface shows the correct status. (Only interfaces on which you explicitly enable unicast RPF display the flag that indicates that unicast RPF is enabled.) The drawback of this approach is that if you want to disable unicast RPF, you must explicitly disable it on every interface. If unicast RPF is enabled on any interface, it is implicitly enabled on all interfaces.

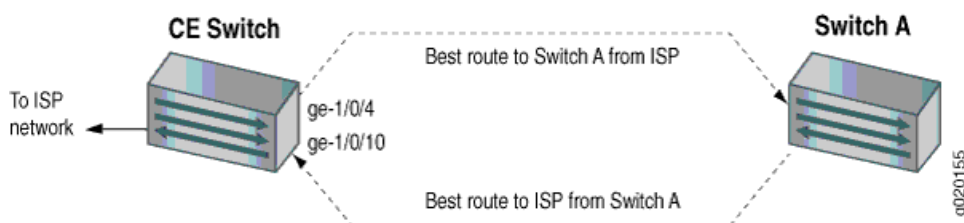
When Not to Enable Unicast RPF

Typically, you will not enable unicast RPF if:

- Switch interfaces are multihomed.
- Switch interfaces are trusted interfaces.
- BGP is carrying prefixes and some of those prefixes are not advertised or are not accepted by the ISP under its policy. (The effect in this case is the same as filtering an interface by using an incomplete access list.)
- Switch interfaces face the network core. Core-facing interfaces are usually asymmetrically routed.

An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination, as shown in [Figure 40 on page 587](#). This means that if an interface receives a packet, that interface does not match the forwarding table entry as the best return path back to the source. If the receiving interface is not the best return path to the source of a packet, unicast RPF causes the switch to discard the packet even though it comes from a valid source.

Figure 40: Asymmetrically Routed Interfaces



NOTE: Do not enable unicast RPF on EX3200, EX4200, and EX4300 switches if any switch interfaces are asymmetrically routed, because unicast RPF is enabled globally on all interfaces of these switches. All switch interfaces must be symmetrically routed for you to enable unicast RPF without the risk of the switch discarding traffic that you want to forward.

Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches

On EX3200, EX4200, and EX4300 switches, the switch implements unicast RPF on a global basis. You cannot enable unicast RPF on a per-interface basis. Unicast RPF is globally disabled by default.

- When you enable unicast RPF on any interface, it is automatically enabled on all switch interfaces, including link aggregation groups (LAGs), integrated routing and bridging (IRB) interfaces, and routed VLAN interfaces (RVIs).
- When you disable unicast RPF on the interface (or interfaces) on which you enabled unicast RPF, it is automatically disabled on all switch interfaces.



NOTE: You must explicitly disable unicast RPF on every interface on which it was explicitly enabled or unicast RPF remains enabled on all switch interfaces.

QFX switches, OCX switches, and EX3200 and EX4200 switches do not perform unicast RPF filtering on equal-cost multipath (ECMP) traffic. The unicast RPF check examines only one best return path to the packet source, but ECMP traffic employs an address block consisting of multiple paths. Using unicast RPF to filter ECMP traffic on these switches can result in the switch discarding packets that you want to forward because the unicast RPF filter does not examine the entire ECMP address block.

Related Documentation

- [Example: Configuring Unicast RPF \(On a Switch\) on page 598](#)
- [Troubleshooting Unicast RPF](#)

Understanding Unicast RPF (Routers)

For interfaces that carry IPv4 or IPv6 traffic, you can reduce the impact of denial of service (DoS) attacks by configuring unicast reverse path forwarding (RPF). Unicast RPF helps determine the source of attacks and rejects packets from unexpected source addresses on interfaces where unicast RPF is enabled.

**NOTE:**

- You can protect a network by applying unicast RPF check feature at the edge (on customer facing interfaces) of the network. In an ISP environment, this can impact the network which can impose on a scaled setup. In case if you have already protected the edge of your network, a packet with a spoofed IP source address would not even appear in a core facing interface. In this case, unicast RPF check is not necessary. Enabling unicast RPF feature can impact the control plane performance, so use it where it is required. So it is strongly recommended not to enable this feature on the network core (internal) interfaces.

- [Unicast RPF and Default Route on page 589](#)
- [Configuring Unicast RPF Strict Mode on page 591](#)
- [Configuring Unicast RPF Loose Mode on page 593](#)
- [Configuring Unicast RPF Loose Mode with Ability to Discard Packets on page 595](#)
- [Configuring Unicast RPF on a VPN on page 596](#)
- [Configuring Unicast RPF on page 597](#)

Unicast RPF and Default Route

When the active route cannot be chosen from the routes in a routing table, the router chooses a default route. A default route is equivalent to an IP address of 0.0.0.0/0. If you configure a default route, and you configure unicast RPF on an interface that the default route uses, unicast RPF behaves differently than it does otherwise. For information about configuring default routes, see the *Junos OS Routing Protocols Library*.

To determine whether the default route uses an interface, enter the **show route** command:

```
user@host> show route address
```

address is the next-hop address of the configured default route. The default route uses the interfaces shown in the output of the **show route** command.

The following sections describe how unicast RPF behaves when a default route uses an interface and when a default route does not use an interface:

- [Unicast RPF Behavior with a Default Route on page 590](#)
- [Unicast RPF Behavior Without a Default Route on page 590](#)
- [Unicast RPF with Routing Asymmetry on page 591](#)

Unicast RPF Behavior with a Default Route

On all routers except those with MPCs and the MX80 router, unicast RPF behaves as follows if you configure a default route that uses an interface configured with unicast RPF:

- Loose mode—All packets are automatically accepted. For this reason, we recommend that you not configure unicast RPF loose mode on interfaces that the default route uses.
- Strict mode—The packet is accepted when the source address of the packet matches any of the routes (either default or learned) that can be reachable through the interface. Note that routes can have multiple destinations associated with them; therefore, if one of the destinations matches the incoming interface of the packet, the packet is accepted.

On all routers with MPCs and the MX80 router, unicast RPF behaves as follows if you configure a default route that uses an interface configured with unicast RPF:

- Loose mode—All packets except the packets whose source is learned from the default route are accepted. All packets whose source is learned from the default route are dropped at the Packet Forwarding Engine. The default route is treated as if the route does not exist.
- Strict mode—The packet is accepted when the source address of the packet matches any of the routes (either default or learned) that can be reachable through the interface. Note that routes can have multiple destinations associated with them; therefore, if one of the destinations matches the incoming interface of the packet, the packet is accepted.

On all routers, the packet is not accepted when either of the following is true:

- The source address of the packet does not match a prefix in the routing table.
- The interface does not expect to receive a packet with this source address prefix.

Unicast RPF Behavior Without a Default Route

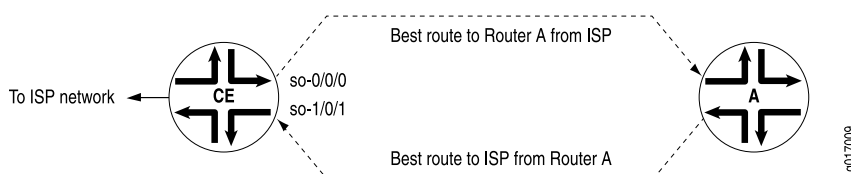
If you do not configure a default route, or if the default route does not use an interface configured with unicast RPF, unicast RPF behaves as described in [“Configuring Unicast RPF Strict Mode” on page 591](#) and [“Configuring Unicast RPF Loose Mode” on page 593](#). To summarize, unicast RPF without a default route behaves as follows:

- Strict mode—The packet is not accepted when either of the following is true:
 - The packet has a source address that does not match a prefix in the routing table.
 - The interface does not expect to receive a packet with this source address prefix.
- Loose mode—The packet is not accepted when the packet has a source address that does not match a prefix in the routing table.

Unicast RPF with Routing Asymmetry

In general, we recommend that you not enable unicast RPF on interfaces that are internal to the network because internal interfaces are likely to have *routing asymmetry*. Routing asymmetry means that a packet's outgoing and return paths are different. Routers in the core of the network are more likely to have asymmetric reverse paths than routers at the customer or provider edge. [Figure 41 on page 591](#) shows unicast RPF in an environment with routing asymmetry.

Figure 41: Unicast RPF with Routing Asymmetry



In [Figure 41 on page 591](#), if you enable unicast RPF on interface `so-0/0/0`, traffic destined for Router A is not rejected. If you enable unicast RPF on interface `so-1/0/1`, traffic from Router A is rejected.

If you need to enable unicast RPF in an asymmetric routing environment, you can use fail filters to allow the router to accept incoming packets that are known to be arriving by specific paths. For an example of a fail filter that accepts packets with a specific source and destination address, see [“Configuring Unicast RPF” on page 597](#).

Configuring Unicast RPF Strict Mode

In strict mode, unicast RPF checks whether the incoming packet has a source address that matches a prefix in the routing table, and whether the interface expects to receive a packet with this source address prefix.

If the incoming packet fails the unicast RPF check, the packet is not accepted on the interface. When a packet is not accepted on an interface, unicast RPF counts the packet and sends it to an optional fail filter. If the fail filter is not configured, the default action is to silently discard the packet.

The optional fail filter allows you to apply a filter to packets that fail the unicast RPF check. You can define the fail filter to perform any filter operation, including accepting, rejecting, logging, sampling, or policing.

When unicast RPF is enabled on an interface, Bootstrap Protocol (BOOTP) packets and Dynamic Host Configuration Protocol (DHCP) packets are not accepted on the interface. To allow the interface to accept BOOTP packets and DHCP packets, you must apply a fail filter that accepts all packets with a source address of `0.0.0.0` and a destination address of `255.255.255.255`. For a configuration example, see [“Configuring Unicast RPF” on page 597](#).

For more information about unicast RPF, see the *Junos OS Routing Protocols Library*. For more information about defining fail filters, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide*.

To configure unicast RPF, include the **rpf-check** statement:

```
rpf-check <fail-filter filter-name>;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family (inet | inet6)]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family (inet | inet6)]

Using unicast RPF can have several consequences when implemented with traffic filters:

- RPF fail filters are evaluated after input filters and before output filters.
- If you configure a filter counter for packets dropped by an input filter, and you want to know the total number of packets dropped, you must also configure a filter counter for packets dropped by the RPF check.
- To count packets that fail the RPF check and are accepted by the RPF fail filter, you must configure a filter counter.
- If an input filter forwards packets anywhere other than the inet.0 or inet6.0 routing tables, the unicast RPF check is not performed.
- If an input filter forwards packets anywhere other than the routing instance the input interface is configured for, the unicast RPF check is not performed.

Configure unicast RPF strict mode, and apply a fail filter that allows the interface to accept BOOTP packets and DHCP packets. The filter accepts all packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255.

To configure unicast RPF in strict mode:

1. Configure the fail filter:

```
[edit firewall]
filter rpf-special-case-dhcp-bootp {
  term allow-dhcp-bootp {
    from {
      source-address {
        0.0.0.0/32;
      }
      address {
        255.255.255.255/32;
      }
    }
    then {
      count rpf-dhcp-bootp-traffic;
      accept;
    }
  }
  term default {
    then {
      log;
    }
  }
}
```

```

    reject;
  }
}

```

2. Configure unicast RPF on interfaces:

```

[edit]
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        rpf-check fail-filter rpf-special-case-dhcp-bootp;
      }
    }
  }
}

```

3. Commit the configuration.

```

[edit]
commit;

```

Configuring Unicast RPF Loose Mode

By default, unicast RPF uses strict mode. Unicast RPF loose mode is similar to unicast RPF strict mode and has the same configuration restrictions. The only check in loose mode is whether the packet has a source address with a corresponding prefix in the routing table; loose mode does not check whether the interface expects to receive a packet with a specific source address prefix. If a corresponding prefix is not found, unicast RPF loose mode does not accept the packet. As in strict mode, loose mode counts the failed packet and optionally forwards it to a fail filter, which either accepts, rejects, logs, samples, or polices the packet.

To configure unicast RPF loose mode, include the **mode**:

1.

```
mode loose;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number* family (inet | inet6) rpf-check <fail-filter *filter-name*>]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family (inet | inet6) rpf-check <fail-filter *filter-name*>]

2. For example:

In this example, no special configuration beyond device initialization is required.

Configure unicast RPF loose mode, and apply a fail filter that allows the interface to accept BOOTP packets and DHCP packets. The filter accepts all packets with a source address of **0.0.0.0** and a destination address of **255.255.255.255**.

To configure unicast RPF in loose mode:

- a. Configure the fail filter:

```
[edit firewall]
filter rpf-special-case-dhcp-bootp {
  term allow-dhcp-bootp {
    from {
      source-address {
        0.0.0.0/32;
      }
      address {
        255.255.255.255/32;
      }
    }
    then {
      count rpf-dhcp-bootp-traffic;
      accept;
    }
  }
  term default {
    then {
      log;
      reject;
    }
  }
}
```

- b. Configure unicast RPF on interfaces:

```
[edit]
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        rpf-check fail-filter rpf-special-case-dhcp-bootp;
        mode loose;
      }
    }
  }
}
```

- c. Commit the configuration.

```
[edit]
commit;
```

Configuring Unicast RPF Loose Mode with Ability to Discard Packets

Starting with Junos OS Release 12.1, unicast RPF loose mode has the ability to discard packets with the source address pointing to the discard interface. This feature is supported on MX Series routers and on T Series routers with Type 1 FPCs, Type 2 FPCs, and Type 3 FPCs. Using unicast RPF loose mode, along with Remote Triggered Black Hole (RTBH) filtering, provides an efficient way to discard packets coming from known attack sources. BGP policies in edge routers ensure that packets with untrusted source addresses have their next hop set to a discard route. When a packet arrives at the router with an untrusted source address, unicast RPF performs a route lookup of the source address. Because the source address route points to a discard next hop, the packet is dropped and a counter is incremented. This feature is supported on both IPv4 (inet) and IPv6 (inet6) address families.

To configure unicast RPF loose mode with the ability to discard packets, include the **rpf-loose-mode-discard family inet** statement at the **[edit forwarding-options]** hierarchy level:

```
rpf-loose-mode-discard {
  family {
    inet;
  }
}
```

In this example, no special configuration beyond device initialization is required.

Configure unicast RPF loose mode, and apply a fail filter that allows the interface to accept BOOTP packets and DHCP packets. The filter accepts all packets with a source address of **0.0.0.0** and a destination address of **255.255.255.255**.

To configure unicast RPF loose mode with the ability to discard packets:

1. Configure the fail filter:

```
[edit firewall]
filter rpf-special-case-dhcp-bootp {
  term allow-dhcp-bootp {
    from {
      source-address {
        0.0.0.0/32;
      }
      address {
        255.255.255.255/32;
      }
    }
    then {
      count rpf-dhcp-bootp-traffic;
      accept;
    }
  }
  term default {
    then {
```

```
    log;
    reject;
  }
}
```

2. Configure unicast RPF on interfaces:

```
[edit]
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        rpf-check fail-filter rpf-special-case-dhcp-bootp;
        mode loose;
      }
    }
  }
}
```

3. Configure the ability to discard packets.

```
[edit]
forwarding-options {
  rpf-loose-mode-discard {
    family {
      inet;
    }
  }
}
```

4. Commit the configuration.

```
[edit]
commit;
```

Configuring Unicast RPF on a VPN

You can configure unicast RPF on a VPN interface by enabling unicast RPF on the interface and including the **interface** statement at the `[edit routing-instances routing-instance-name]` hierarchy level.

You can configure unicast RPF only on the interfaces you specify in the routing instance. This means the following:

- For Layer 3 VPNs, unicast RPF is supported on the CE router interface.
- Unicast RPF is not supported on core-facing interfaces.

- For virtual-router routing instances, unicast RPF is supported on all interfaces you specify in the routing instance.
- If an input filter forwards packets anywhere other than the routing instance the input interface is configured for, the unicast RPF check is not performed.

For more information about VPNs and virtual-router routing instances, see the *Junos OS VPNs Library for Routing Devices*. For more information about FBF, see the *Junos OS Routing Protocols Library*.

Configure unicast RPF on a Layer 3 VPN interface:

```
[edit interfaces]
so-0/0/0 {
  unit 0 {
    family inet {
      rpf-check;
    }
  }
}
[edit routing-instance]
VPN-A {
  interface so-0/0/0.0;
}
```

Configuring Unicast RPF

Configure unicast RPF strict mode, and apply a fail filter that allows the interface to accept BOOTP packets and DHCP packets. The filter accepts all packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255.

```
[edit firewall]
filter rpf-special-case-dhcp-bootp {
  term allow-dhcp-bootp {
    from {
      source-address {
        0.0.0.0/32;
      }
      address {
        255.255.255.255/32;
      }
    }
    then {
      count rpf-dhcp-bootp-traffic;
      accept;
    }
  }
  term default {
    then {
      log;
      reject;
    }
  }
}
```

```
[edit]
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        rpf-check fail-filter rpf-special-case-dhcp-bootp;
      }
    }
  }
}
```

See Also • [unicast-reverse-path](#)

Example: Configuring Unicast RPF (On a Switch)

This example shows how to help defend ingress interfaces against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks by configuring unicast RPF to filter incoming traffic.

- [Requirements on page 598](#)
- [Overview and Topology on page 599](#)
- [Configuration on page 599](#)
- [Disabling Unicast RPF on page 600](#)
- [Verification on page 600](#)
- [Troubleshooting Unicast RPF on page 602](#)

Requirements

This example uses two EX8200 switches. On EX3200 and EX4200 switches, you cannot configure individual interfaces for unicast RPF – the switch applies unicast RPF globally to all interfaces on the switch.

- Junos OS Release 10.1 or later for EX Series switches
- Two EX8200 switches

Before you begin, be sure you have:

- Connected the two switches by symmetrically routed interfaces.
- Ensured that the interface on which you will configure unicast RPF is symmetrically routed.
- On an EX8200, EX6200, QFX Series switch, or OCX Series switch, ensure that the selected switch interface is symmetrically routed before you enable unicast RPF. A symmetrically routed interface is an interface that uses the same route in both directions between the source and the destination. Do not enable unicast RPF on asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination.

- On an EX3200, EX4200, or EX4300 switch, ensure that *all* switch interfaces are symmetrically routed before you enable unicast RPF on an interface. When you enable unicast RPF on any interface, it is enabled globally on all switch interfaces. Do not enable unicast RPF on asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination.

Overview and Topology

In this example, an enterprise network's system administrator wants to protect Switch A against potential DoS and DDoS attacks from the Internet. The administrator configures unicast RPF on interface **ge-1/0/10** on Switch A. Packets arriving on interface **ge-1/0/10** on Switch A from the Switch B source also use incoming interface **ge-1/0/10** as the best return path to send packets back to the source.

The topology of this configuration example uses two EX8200 switches, Switch A and Switch B, connected by symmetrically routed interfaces:

- Switch A is on the edge of an enterprise network. The interface **ge-1/0/10** on Switch A connects to the interface **ge-1/0/5** on Switch B.
- Switch B is on the edge of the service provider network that connects the enterprise network to the Internet.

Configuration

To enable unicast RPF, perform these tasks:

CLI Quick Configuration

To quickly configure unicast RPF on Switch A, copy the following command and paste it into the switch terminal window:

```
[edit interfaces]
set ge-1/0/10 unit 0 family inet rpf-check
```

Step-by-Step Procedure

To configure unicast RPF on Switch A:

1. Enable unicast RPF on interface **ge-1/0/10**:

```
[edit interfaces]
user@switch# set ge-1/0/10 unit 0 family inet rpf-check
```

Results

Check the results:

```
[edit interfaces]
user@switch# show
ge-1/0/10 {
  unit 0 {
    family inet {
      rpf-check;
    }
  }
}
```

```
}
}
```

Disabling Unicast RPF

Verification

Unicast reverse-path forwarding (RPF) can help protect your LAN from denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on untrusted interfaces. Unicast RPF filters traffic with source addresses that do not use the incoming interface as the best return path back to the source. If the network configuration changes so that an interface that has unicast RPF enabled becomes a trusted interface or becomes asymmetrically routed (the interface that receives a packet is not the best return path to the packet's source), disable unicast RPF.

To disable unicast RPF on an EX3200, EX4200, or EX4300 switch, you must delete it from every interface on which you explicitly configured it. If you do not disable unicast RPF on every interface on which you explicitly enabled it, it remains implicitly enabled on all interfaces. If you attempt to delete unicast RPF from an interface on which it was not explicitly enabled, the **warning: statement not found** message appears. If you do not disable unicast RPF on every interface on which you explicitly enabled it, unicast RPF remains implicitly enabled on all interfaces of the EX3200, EX4200, or EX4300 switch.

On EX8200, EX6200, QFX Series switches, and OCX Series switches, the switch does not apply unicast RPF to an interface unless you explicitly enable that interface for unicast RPF.

To disable unicast RPF, delete its configuration from the interface:

```
[edit interfaces]
user@switch# delete ge-1/0/10 unit 0 family inet rpf-check
```

- [Verifying That Unicast RPF Is Enabled on the Switch on page 600](#)

Verifying That Unicast RPF Is Enabled on the Switch

Purpose Verify that unicast RPF is enabled and working on the interface.

Action Use one of the **show interfaces *interface-name*** commands with either the **extensive** or **detail** options to verify that unicast RPF is enabled and working on the switch. The example below displays output from the **show interfaces ge- extensive** command.

```
user@switch> show show interfaces ge-1/0/10 extensive
Physical interface: ge-1/0/10, Enabled, Physical link is Down
Interface index: 139, SNMP ifIndex: 58, Generation: 140
Link-level type: Ethernet, MTU: 1514, Speed: Auto, MAC-REWRITE Error: None,
Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled,
Auto-negotiation: Enabled, Remote fault: Online
Device flags   : Present Running
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
```

```

Link flags      : None
CoS queues     : 8 supported, 8 maximum usable queues
Hold-times     : Up 0 ms, Down 0 ms
Current address: 00:19:e2:50:95:ab, Hardware address: 00:19:e2:50:95:ab
Last flapped   : Never
Statistics last cleared: Never
Traffic statistics:
  Input bytes  :                0                0 bps
  Output bytes :                0                0 bps
  Input packets:                0                0 pps
  Output packets:              0                0 pps
IPv6 transit statistics:
  Input bytes  :                0
  Output bytes :                0
  Input packets:                0
  Output packets:              0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runt: 0, Policed discards: 0,
  L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
  FIFO errors: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,

  FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

  0 best-effort                0                0                0
  1 assured-forw                0                0                0
  5 expedited-fo                0                0                0
  7 network-cont                0                0                0

Active alarms : LINK
Active defects : LINK
MAC statistics:
  Total octets      Receive      Transmit
  Total packets      0            0
  Unicast packets    0            0
  Broadcast packets  0            0
  Multicast packets  0            0
  CRC/Align errors   0            0
  FIFO errors        0            0
  MAC control frames 0            0
  MAC pause frames   0            0
  Oversized frames   0
  Jabber frames      0
  Fragment frames    0
  VLAN tagged frames 0
  Code violations     0
Filter statistics:
  Input packet count      0
  Input packet rejects    0
  Input DA rejects        0
  Input SA rejects        0
  Output packet count      0
  Output packet pad count  0
  Output packet error count 0

```

```

CAM destination filters: 0, CAM source filters: 0
Autonegotiation information:
  Negotiation status: Incomplete
Packet Forwarding Engine configuration:
  Destination slot: 1

Logical interface ge-1/0/10.0 (Index 69) (SNMP ifIndex 59) (Generation 135)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
IPv6 transit statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps
IPv6 transit statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
  Protocol inet, Generation: 144, Route table: 0
Flags: uRPF
Addresses, Flags: Is-Preferred Is-Primary

```

Meaning The `show interfaces ge-1/0/10 extensive` command (and the `show interfaces ge-1/0/10 detail` command) displays in-depth information about the interface. The **Flags:** output field near the bottom of the display reports the unicast RPF status. If unicast RPF has not been enabled, the **uRPF** flag is not displayed.

On EX3200 and EX4200 switches, unicast RPF is implicitly enabled on *all* switch interfaces, including aggregated Ethernet interfaces (also referred to as link aggregation groups or LAGs) and routed VLAN interfaces (RVIs) when you enable unicast RPF on a single interface. However, the unicast RPF status is shown as enabled only on interfaces for which you have explicitly configured unicast RPF. Thus, the **uRPF** flag is not displayed on interfaces for which you have not explicitly configured unicast RPF even though unicast RPF is implicitly enabled on all interfaces on EX3200 and EX4200 switches.

Troubleshooting Unicast RPF

- [Legitimate Packets Are Discarded on page 603](#)

Legitimate Packets Are Discarded

Problem The switch filters valid packets from legitimate sources, which results in the switch's discarding packets that should be forwarded.

Solution The interface or interfaces on which legitimate packets are discarded are asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination, so the interface that receives a packet is not the same interface the switch uses to reply to the packet's source.

Unicast RPF works properly only on symmetrically routed interfaces. A symmetrically routed interface is an interface that uses the same route in both directions between the source and the destination. Unicast RPF filters packets by checking the forwarding table for the best return path to the source of an incoming packet. If the best return path uses the same interface as the interface that received the packet, the switch forwards the packet. If the best return path uses a different interface than the interface that received the packet, the switch discards the packet.



NOTE: On EX3200, EX4200, and EX4300 switches, unicast RPF works properly only if all switch interfaces—including aggregated Ethernet interfaces (also referred to as link aggregation groups or LAGs), integrated routing and bridging (IRB) interfaces, and routed VLAN interfaces (RVIs)—are symmetrically routed, because unicast RPF is enabled globally on all switch interfaces.

Related Documentation

- [Understanding Unicast RPF \(Switches\) on page 584](#)

Example: Configuring Unicast RPF (On a Router)

This example shows how to help defend ingress interfaces against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks by configuring unicast RPF on a customer-edge interface to filter incoming traffic.

- [Requirements on page 603](#)
- [Overview on page 604](#)
- [Configuration on page 604](#)
- [Verification on page 610](#)

Requirements

No special configuration beyond device initialization is required.

Overview

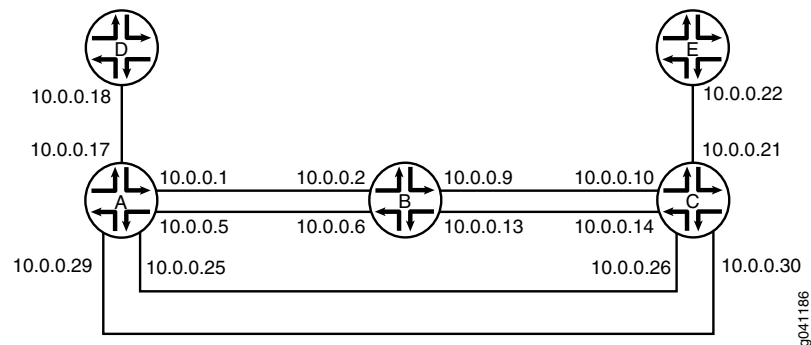
In this example, Device A is using OSPF to advertise a prefix for the link that connects to Device D. Device B has unicast RPF configured. OSPF is enabled on the links between Device B and Device C and the links between Device A and Device C, but not on the links between Device A and Device B. Therefore, Device B learns about the route to Device D through Device C.

If ingress filtering is used in an environment where DHCP or BOOTP is used, it should be ensured that the packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255 are allowed to reach the relay agent in routers when appropriate.

This example also includes a fail filter. When a packet fails the unicast RPF check, the fail filter is evaluated to determine if the packet should be accepted anyway. The fail filter in this example allows Device B's interfaces to accept Dynamic Host Configuration Protocol (DHCP) packets. The filter accepts all packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255.

Figure 42 on page 604 shows the sample network.

Figure 42: Unicast RPF Sample Topoolgy



Configuration

CLI Quick Configuration

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

Device A

```

set interfaces fe-1/2/0 unit 1 family inet address 10.0.0.1/30
set interfaces fe-0/0/2 unit 5 family inet address 10.0.0.5/30
set interfaces fe-0/0/1 unit 17 family inet address 10.0.0.17/30
set interfaces fe-0/1/1 unit 25 family inet address 10.0.0.25/30
set interfaces fe-1/1/1 unit 29 family inet address 10.0.0.29/30
set protocols ospf export send-direct
set protocols ospf area 0.0.0.0 interface fe-0/1/1.25
set protocols ospf area 0.0.0.0 interface fe-1/1/1.29
set policy-options policy-statement send-direct from protocol direct
set policy-options policy-statement send-direct from route-filter 10.0.0.16/30 exact
set policy-options policy-statement send-direct then accept
  
```


Device B	<pre> set interfaces fe-1/2/0 unit 2 family inet rpf-check fail-filter rpf-special-case-dhcp set interfaces fe-1/2/0 unit 2 family inet address 10.0.0.2/30 set interfaces fe-1/1/1 unit 6 family inet rpf-check fail-filter rpf-special-case-dhcp set interfaces fe-1/1/1 unit 6 family inet address 10.0.0.6/30 set interfaces fe-0/1/1 unit 9 family inet rpf-check fail-filter rpf-special-case-dhcp set interfaces fe-0/1/1 unit 9 family inet address 10.0.0.9/30 set interfaces fe-0/1/0 unit 13 family inet rpf-check fail-filter rpf-special-case-dhcp set interfaces fe-0/1/0 unit 13 family inet address 10.0.0.13/30 set protocols ospf area 0.0.0.0 interface fe-0/1/1.9 set protocols ospf area 0.0.0.0 interface fe-0/1/0.13 set routing-options forwarding-table unicast-reverse-path active-paths set firewall filter rpf-special-case-dhcp term allow-dhcp from source-address 0.0.0.0/32 set firewall filter rpf-special-case-dhcp term allow-dhcp from destination-address 255.255.255.255/32 set firewall filter rpf-special-case-dhcp term allow-dhcp then count rpf-dhcp-traffic set firewall filter rpf-special-case-dhcp term allow-dhcp then accept set firewall filter rpf-special-case-dhcp term default then log set firewall filter rpf-special-case-dhcp term default then reject </pre>
Device C	<pre> set interfaces fe-1/2/0 unit 10 family inet address 10.0.0.10/30 set interfaces fe-0/0/2 unit 14 family inet address 10.0.0.14/30 set interfaces fe-1/0/2 unit 21 family inet address 10.0.0.21/30 set interfaces fe-1/2/2 unit 26 family inet address 10.0.0.26/30 set interfaces fe-1/2/1 unit 30 family inet address 10.0.0.30/30 set protocols ospf area 0.0.0.0 interface fe-1/2/0.10 set protocols ospf area 0.0.0.0 interface fe-0/0/2.14 set protocols ospf area 0.0.0.0 interface fe-1/2/2.26 set protocols ospf area 0.0.0.0 interface fe-1/2/1.30 </pre>
Device D	<pre> set interfaces fe-1/2/0 unit 18 family inet address 10.0.0.18/30 </pre>
Device E	<pre> set interfaces fe-1/2/0 unit 22 family inet address 10.0.0.22/30 </pre>

Configuring Device A

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*.

To configure Device A:

1. Configure the interfaces.

```

[edit interfaces]
user@A# set fe-1/2/0 unit 1 family inet address 10.0.0.1/30
user@A# set fe-0/0/2 unit 5 family inet address 10.0.0.5/30
user@A# set fe-0/0/1 unit 17 family inet address 10.0.0.17/30
user@A# set fe-0/1/1 unit 25 family inet address 10.0.0.25/30
user@A# set fe-1/1/1 unit 29 family inet address 10.0.0.29/30

```

2. Configure OSPF.

```
[edit protocols ospf]
user@A# set export send-direct
user@A# set area 0.0.0.0 interface fe-0/1/1.25
user@A# set area 0.0.0.0 interface fe-1/1/1.29
```

3. Configure the routing policy.

```
[edit policy-options policy-statement send-direct]
user@A# set from protocol direct
user@A# set from route-filter 10.0.0.16/30 exact
user@A# set then accept
```

4. If you are done configuring Device A, commit the configuration.

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

Configuring Device B

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*.

To configure Device B:

1. Configure the interfaces.

```
[edit interfaces]
user@B# set fe-1/2/0 unit 2 family inet address 10.0.0.2/30
user@B# set fe-1/1/1 unit 6 family inet address 10.0.0.6/30
user@B# set fe-0/1/1 unit 9 family inet address 10.0.0.9/30
user@B# set fe-0/1/0 unit 13 family inet address 10.0.0.13/30
```

2. Configure OSPF.

```
[edit protocols ospf area 0.0.0.0]
user@B# set interface fe-0/1/1.9
user@B# set interface fe-0/1/0.13
```

3. Configure unicast RPF, and apply the optional fail filter.

```
[edit interfaces]
user@B# set fe-1/2/0 unit 2 family inet rpf-check fail-filter rpf-special-case-dhcp
user@B# set fe-1/1/1 unit 6 family inet rpf-check fail-filter rpf-special-case-dhcp
user@B# set fe-0/1/1 unit 9 family inet rpf-check fail-filter rpf-special-case-dhcp
user@B# set fe-0/1/0 unit 13 family inet rpf-check fail-filter rpf-special-case-dhcp
```

4. (Optional) Configure the fail filter that gets evaluated if a packet fails the RPF check.

```
[edit firewall filter rpf-special-case-dhcp]
user@B# set term allow-dhcp from source-address 0.0.0.0/32
user@B# set term allow-dhcp from destination-address 255.255.255.255/32
user@B# set term allow-dhcp then count rpf-dhcp-traffic
user@B# set term allow-dhcp then accept
user@B# set term default then log
user@B# set term default then reject
```

5. (Optional) Configure only active paths to be considered in the RPF check.

This is the default behavior.

```
[edit routing-options forwarding-table]
user@B# set unicast-reverse-path active-paths
```

6. If you are done configuring Device B, commit the configuration.

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

Results

Confirm your configuration by issuing the **show firewall**, **show interfaces**, **show protocols**, **show routing-options**, and **show policy-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Device A

```
user@A# show interfaces
fe-1/2/0 {
  unit 1 {
    family inet {
      address 10.0.0.1/30;
    }
  }
}
fe-0/0/2 {
  unit 5 {
    family inet {
      address 10.0.0.5/30;
    }
  }
}
fe-0/0/1 {
  unit 17 {
    family inet {
      address 10.0.0.17/30;
    }
  }
}
```

```
}
fe-0/1/1 {
  unit 25 {
    family inet {
      address 10.0.0.25/30;
    }
  }
}
fe-1/1/1 {
  unit 29 {
    family inet {
      address 10.0.0.29/30;
    }
  }
}
```

```
user@A# show protocols
ospf {
  export send-direct;
  area 0.0.0.0 {
    interface fe-0/1/1.25;
    interface fe-1/1/1.29;
  }
}
```

```
user@A# show policy-options
policy-statement send-direct {
  from {
    protocol direct;
    route-filter 10.0.0.16/30 exact;
  }
  then accept;
}
```

Device B

```
user@B# show firewall
filter rpf-special-case-dhcp {
  term allow-dhcp {
    from {
      source-address {
        0.0.0.0/32;
      }
      destination-address {
        255.255.255.255/32;
      }
    }
    then {
      count rpf-dhcp-traffic;
      accept;
    }
  }
  term default {
    then {
```

```
        log;
        reject;
    }
}
}
user@B# show interfaces
fe-1/2/0 {
    unit 2 {
        family inet {
            rpf-check fail-filter rpf-special-case-dhcp;
            address 10.0.0.2/30;
        }
    }
}
fe-1/1/1 {
    unit 6 {
        family inet {
            rpf-check fail-filter rpf-special-case-dhcp;
            address 10.0.0.6/30;
        }
    }
}
fe-0/1/1 {
    unit 9 {
        family inet {
            rpf-check fail-filter rpf-special-case-dhcp;
            address 10.0.0.9/30;
        }
    }
}
fe-0/1/0 {
    unit 13 {
        family inet {
            rpf-check fail-filter rpf-special-case-dhcp;
            address 10.0.0.13/30;
        }
    }
}
```

```
user@B# show protocols
ospf {
    area 0.0.0.0 {
        interface fe-0/1/1.9;
        interface fe-0/1/0.13;
    }
}
```

```
user@B# show routing-options
forwarding-table {
    unicast-reverse-path active-paths;
}
```

Enter the configurations on Device C, Device D, and Device E, as shown in “[CLI Quick Configuration](#)” on page 604.

Verification

Confirm that the configuration is working properly.

- [Confirm That Unicast RPF Is Enabled](#) on page 610
- [Confirm That the Source Addresses Are Blocked](#) on page 610
- [Confirm That the Source Addresses Are Unblocked](#) on page 611

Confirm That Unicast RPF Is Enabled

Purpose Make sure that the interfaces on Device B have unicast RPF enabled.

Action user@B> show interfaces fe-0/1/0.13 extensive

```
Logical interface fe-0/1/0.13 (Index 73) (SNMP ifIndex 553) (Generation 208)
Flags: SNMP-Traps 0x4000 Encapsulation: ENET2
Traffic statistics:
  Input bytes :          999390
  Output bytes :         1230122
  Input packets:          12563
  Output packets:         12613
Local statistics:
  Input bytes :          998994
  Output bytes :         1230122
  Input packets:          12563
  Output packets:         12613
Transit statistics:
  Input bytes :           396          0 bps
  Output bytes :           0          0 bps
  Input packets:           0          0 pps
  Output packets:          0          0 pps
Protocol inet, MTU: 1500, Generation: 289, Route table: 22
  Flags: Sendbcst-pkt-to-re, uRPF
  RPF Failures: Packets: 0, Bytes: 0
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.0.0.12/30, Local: 10.0.0.13, Broadcast: 10.0.0.15,
  Generation: 241
```

Meaning The **uRPF** flag confirms that unicast RPF is enabled on this interface.

Confirm That the Source Addresses Are Blocked

Purpose Use the **ping** command to make sure that Device B blocks traffic from unexpected source addresses.

Action From Device A, ping Device B's interfaces, using 10.0.0.17 as the source address.

```
user@A> ping 10.0.0.6 source 10.0.0.17
PING 10.0.0.6 (10.0.0.6): 56 data bytes
^C
--- 10.0.0.6 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
```

Meaning As expected, the ping operation fails.

Confirm That the Source Addresses Are Unblocked

Purpose Use the **ping** command to make sure that Device B does not block traffic when the RPF check is deactivated.

Action

1. Deactivate the RPF check on one of the interfaces.
2. Rerun the ping operation.

```
user@B> deactivate interfaces fe-1/1/1.6 family inet rpf-check

user@A> ping 10.0.0.6 source 10.0.0.17
PING 10.0.0.2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=63 time=1.316 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=63 time=1.263 ms
^C
--- 10.0.0.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.263/1.289/1.316/0.027 ms
```

Meaning As expected, the ping operation succeeds.

Unknown Unicast Forwarding

- [Understanding and Preventing Unknown Unicast Forwarding on page 613](#)

Understanding and Preventing Unknown Unicast Forwarding

Unknown unicast traffic consists of unicast packets with unknown destination MAC addresses. By default, the switch floods these unicast packets that traverse a VLAN to all interfaces that are members of that VLAN. Forwarding this type of traffic can create unnecessary traffic that leads to poor network performance or even a complete loss of network service. This flooding of packets is known as a traffic storm.

To prevent a traffic storm, you can disable the flooding of unknown unicast packets to all VLAN interfaces by configuring specific VLANs or all VLANs to forward all unknown unicast traffic traversing them to a specific interface. You can configure multiple VLANs to forward unknown unicast packets to the same interface or configure different interfaces for different VLANs. This channels the unknown unicast traffic traversing VLANs to specific interfaces instead of flooding all interfaces.

- [Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface on page 613](#)
- [Configuring Unknown Unicast Forwarding \(ELS\) on page 614](#)
- [Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 617](#)
- [Configuring Unknown Unicast Forwarding \(CLI Procedure\) on page 618](#)

Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface

Purpose Verify that a VLAN is forwarding all unknown unicast packets (those with unknown destination MAC addresses) to a single interface instead of flooding unknown unicast packets across all interfaces that are members of that VLAN.



NOTE: This procedure uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, See: [“Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface” on page 617](#). For ELS details see: *Using the Enhanced Layer 2 Software CLI*.

Action (EX4300 Switches) Display the forwarding interface for unknown unicast packets for a VLAN (here, the VLAN name is v1):

```
user@switch> show configuration switch-options
```

```
unknown-unicast-forwarding {
  vlan v1 {
    interface ge-0/0/7.0;
  }
}
```

(EX9200 Switches) Display the forwarding interface for unknown unicast packets:

```
user@switch> show forwarding-options
```

```
next-hop-group uuf-nhg {
  group-type layer-2;
  interface ge-0/0/7.0;
}
```

Meaning The sample output from the **show** commands show that the unknown unicast forwarding interface for VLAN v1 is interface **ge-0/0/7**.

Configuring Unknown Unicast Forwarding (ELS)



NOTE: This task uses Junos OS for EX Series switches or QFX Series with support for the Enhanced Layer 2 Software (ELS) configuration style. If your EX Series switch runs software that does not support ELS, see [“Configuring Unknown Unicast Forwarding \(CLI Procedure\)” on page 618](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*

Unknown unicast traffic consists of packets with unknown destination MAC addresses. By default, the switch floods these packets that traverse a VLAN to all interfaces associated with that VLAN. This flooding of packets is known as a traffic storm and can negatively impact network performance.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN to a specific interface. You can configure each VLAN to divert unknown unicast traffic to a different interface or use the same interface for multiple VLANs.

- [Configuring Unknown Unicast Forwarding on EX4300 Switches on page 615](#)
- [Configuring Unknown Unicast Forwarding on EX9200 Switches on page 615](#)

Configuring Unknown Unicast Forwarding on EX4300 Switches

To configure unknown unicast forwarding options on EX4300 switches:

- Configure unknown unicast forwarding for a specific VLAN and specify the interface to which all unknown unicast traffic will be forwarded:

```
[edit switch-options]
user@switch# set unknown-unicast-forwarding vlan vlan-name interface interface-name
```

- Configure unknown unicast forwarding for all VLANs and specify the interface to which all unknown unicast traffic will be forwarded:

```
[edit switch-options]
user@switch# set unknown-unicast-forwarding vlan all interface interface-name
```

Configuring Unknown Unicast Forwarding on EX9200 Switches

To configure unknown unicast forwarding on EX9200 switches, you must configure a flood filter and apply it to VLANs for which you want to configure unknown unicast forwarding. Flood filters are firewall filters that are applied only to broadcast, unknown unicast, and multicast (BUM) traffic. If a flood filter is configured, only traffic packets that are of the packet type **unknown-unicast** are forwarded to the interface on which unicast forwarding is configured. A next-hop group redirects the packets according to the action specified in the flood filter.

To configure the next-hop group that receives Layer 2 packets and then configure the interface to which these packets are forwarded:

1. Configure the **next-hop-group** action for the Layer 2 interface expected to receive unknown unicast packets:

```
[edit forwarding-options]
user@switch# set next-hop-group next-hop-group-name group-type layer-2
[edit forwarding-options]
user@switch# set next-hop-group next-hop-group-name interface interface-name
```

For example:

```
[edit forwarding-options]
user@switch# set next-hop-group uuf-nhg group-type layer-2
[edit forwarding-options]
user@switch# set next-hop-group uuf-nhg interface ge-3/1/7.0
```

2. Configure a firewall filter with family address type **ethernet-switching**:

```
[edit firewall]
user@switch# set family ethernet-switching filter filter-name
```

For example:

```
[edit firewall]
user@switch# set family ethernet-switching filter uuf_filter
```

3. Configure a term in the firewall filter for the interface that receives unknown unicast packets (the interface specified in Step 1) to discard unknown unicast packets:

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name from interface interface-name
user@switch# set term term-name from traffic-type unknown-unicast
user@switch# set term term-name then discard
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term source-drop from interface ge-3/1/7.0
user@switch# set term source-drop from traffic-type unknown-unicast
user@switch# set term source-drop then discard
```

4. Configure a term in the firewall filter for unknown unicast packets to be flooded to the interface enabled for unknown unicast forwarding by using **next-hop-group** (in step 1):

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name from traffic-type unknown-unicast
user@switch# set term term-name then next-hop-group group-name
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term uuf-flood from traffic-type unknown-unicast
user@switch# set term uuf-flood then next-hop-group uuf-nhg
```

5. Configure a default term for the firewall filter to forward packets other than unknown unicast packets:

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name then accept
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term fwd-default then accept
```

6. Apply the filter as a flood filter on the VLAN that includes the interface which will receive unknown unicast packets:

```
[edit vlans vlan-name]
user@switch# set forwarding-options flood input filter-name
```

For example:

```
[edit vlans v1]
user@switch# set forwarding-options flood input uuf_filter
```

Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface

Purpose Verify that a VLAN is forwarding all unknown unicast packets (those with unknown destination MAC addresses) to a single trunk interface instead of flooding unknown unicast packets across all interfaces that are members of the same VLAN.

Action Display the forwarding interface for unknown unicast packets for a VLAN (here, the VLAN name is **v1**):

```
user@switch> show configuration ethernet-switching-options
```

```
unknown-unicast-forwarding {
  vlan v1 {
    interface ge-0/0/7.0;
  }
}
```

Display the Ethernet switching table:

```
user@switch> show ethernet-switching table vlan v1
```

```
Ethernet-switching table: 3 unicast entries
VLAN      MAC address      Type      Age  Interfaces
v1         *                Flood     -    All-members
v1         00:01:09:00:00:00 Learn     24   ge-0/0/7.0
v1         00:11:09:00:01:00 Learn     37   ge-0/0/3.0
```

Meaning The sample output from the **show configuration ethernet-switching-options** command shows that the unknown unicast forwarding interface for VLAN **v1** is interface **ge-0/0/7**. The **show ethernet-switching table** command shows that an unknown unicast packet is received on interface **ge-0/0/3** with the destination MAC address (DMAC) **00:01:09:00:00:00** and the source MAC address (SMAC) of **00:11:09:00:01:00**. This shows that the SMAC of the packet is learned in the normal way (through the interface **ge-0/0/3.0**), while the DMAC is learned on interface **ge-0/0/7**.

See Also

Configuring Unknown Unicast Forwarding (CLI Procedure)

Unknown unicast traffic consists of packets with unknown destination MAC addresses. By default, the switch floods these packets to all interfaces associated with a VLAN. Forwarding such traffic to interfaces on the switch can create a security issue.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN out to a specific trunk interface. From there, the destination MAC address can be learned and added to the Ethernet switching table. You can configure each VLAN to divert unknown unicast traffic to different trunk interfaces or use one trunk interface for multiple VLANs.



NOTE: For Junos OS for EX Series switches or QFX Series with support for the Enhanced Layer 2 Software (ELS) configuration style, see [“Configuring Unknown Unicast Forwarding \(ELS\)” on page 614](#).

To configure unknown unicast forwarding options:



NOTE: Before you can configure unknown unicast forwarding within a VLAN, you must first configure that VLAN.

1. Configure unknown unicast forwarding for a specific VLAN (here, the VLAN name is **employee**):

```
[edit ethernet-switching-options]
user@switch# set unknown-unicast-forwarding vlan employee
```

2. Specify the trunk interface to which all unknown unicast traffic will be forwarded:

```
[edit ethernet-switching-options]
user@switch# set unknown-unicast-forwarding vlan employee interface ge-0/0/3.0
```

Related Documentation

- [Understanding and Preventing Unknown Unicast Forwarding on page 613](#)
- [Understanding Storm Control on page 622](#)
- [Configuring Autorecovery for Port Security Events on page 635](#)

PART 12

Storm Control

- [Understanding and Using Storm Control on page 621](#)

CHAPTER 26

Understanding and Using Storm Control

- [Understanding Storm Control on page 622](#)
- [Enabling and Disabling Storm Control \(non-ELS\) on page 626](#)
- [Enabling and Disabling Storm Control \(ELS\) on page 630](#)
- [Configuring Autorecovery for Port Security Events on page 635](#)
- [Example: Using Storm Control to Prevent Network Outages on page 636](#)

Understanding Storm Control

A traffic storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect. The LAN is suddenly flooded with packets, creating unnecessary traffic that leads to poor network performance or even a complete loss of network service. Storm control enables the switch to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the *storm control level*—is exceeded, thus preventing packets from proliferating and degrading the LAN. As an alternative to having the switch drop packets, you can configure it to shut down interfaces or temporarily disable interfaces (see the [action-shutdown](#) statement or the [port-error-disable](#) statement) when the storm control level is exceeded.

To recognize a storm, you must be able to identify when traffic has reached an abnormal level. Suspect a storm when operations begin timing out and network response times slow down. Users might be unable to access expected services. Monitor the percentage of broadcast and unknown unicast traffic in the network when it is operating normally. This data can then be used as a benchmark to determine when traffic levels are too high. You can then configure storm control to set the level at which you want to drop broadcast and unknown unicast traffic.



CAUTION: The Junos OS allows you to configure a storm control value that exceeds the bandwidth of the interface. If you configure an interface this way, storm control does not drop broadcast or unknown unicast packets even if they consume all the available bandwidth.

Storm control is enabled by default on ELS platforms and disabled by default on non-ELS platforms. If storm control is enabled, the default level is 80 percent of the available bandwidth for ingress traffic. You can change the storm control level by configuring it as a specific bandwidth value. (The **level** configuration statement, which allows you to configure the storm control level as a percentage of the combined broadcast and unknown unicast streams, is deprecated and might be removed from future releases. We recommend that you phase out its use and replace it with the **bandwidth** statement.)

You can customize the storm control level for a specific interface by explicitly configuring either **bandwidth** or **level** (but not both at the same time for the same interface).

- **bandwidth level**—Configures the storm control level as the bandwidth in kilobits per second of the applicable traffic streams on that interface.
- **Bandwidth percentage**—Configures the storm control level as a percentage of the available bandwidth used by the combined applicable traffic streams that are subject to storm control on that interface.

When you configure storm control bandwidth or storm control level on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth or level. For example, if you configure a storm control bandwidth of 15,000 Kbps on **ae1**, and **ae1** has two members, **ge-0/0/0** and **ge-0/0/1**, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on **ae1** allows a traffic rate of up to 30,000 Kbps of combined traffic streams. Traffic might

include broadcast, multicast, and unknown unicast traffic, depending upon the configuration.

The sending and receiving of broadcast, multicast, and unicast packets are part of normal LAN operation, so to recognize a storm, you must be able to identify when traffic has reached a level that is abnormal for your LAN. Suspect a storm when operations begin timing out and network response times slow down. As more packets flood the LAN, network users might be unable to access servers or e-mail.

Monitor the level of broadcast, multicast, and unknown unicast traffic in the LAN when it is operating normally. Use this data as a benchmark to determine when traffic levels are too high. Then configure storm control to set the level at which you want to drop broadcast traffic, multicast traffic, unknown unicast traffic, or two or all three of those traffic types.

You can change the storm control level for a specific interface by configuring the bandwidth value or the storm control level for the combined traffic streams that are subject to storm control on that interface. The type of traffic stream (broadcast, unknown unicast, and multicast) that is included within the bandwidth or storm control level consideration depends on which types of traffic are enabled for storm control monitoring on that interface.

You can disable the storm control selectively for broadcast, multicast, or unknown unicast traffic, or any combination of traffic types. When disabling storm control for multicast traffic, you can specify the traffic to be either registered multicast or unregistered multicast. Registered multicast MAC addresses are multicast MAC addresses that are within the range 01-00-5E-00-00-00 through 01-00-5E-7F-FF-FF (multicast MAC addresses outside this range are called unregistered multicast addresses).



NOTE: On an FCoE-FC gateway, storm control must be disabled on all Ethernet interfaces that belong to an FCoE VLAN to prevent FCoE traffic from being dropped. Configuring storm control on an Ethernet interface that is included in an FCoE-FC gateway may have undesirable effects, including FCoE packet loss. After disabling storm control on all interfaces, enable storm control on any interfaces that are not part of an FCoE-FC gateway on which you want to use storm control. However, on an FCoE transit switch, you can enable storm control on interfaces that carry FCoE traffic.

- You can enable storm control selectively for multicast traffic on a specific interface or on all interfaces.
- On all switches—You can disable storm control selectively for either broadcast streams, or multicast streams, or for unknown unicast streams.
- On EX8200 switches—You can also disable storm control selectively for either registered multicast traffic, or unregistered multicast traffic, or for both types of multicast traffic.

The default configuration of storm control differs according to the switch line:

- On EX2200, EX3200, EX3300, EX4200, and EX6200 access ports—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control for broadcast and unknown unicast traffic on all switch interfaces, with the storm control level set to 80 percent of the available bandwidth used by the broadcast and unknown unicast traffic streams.
- On EX4300, EX4500, and EX8200 switches—The factory default configuration enables storm control on all switch interfaces, with the storm control level set to 80 percent of the combined broadcast, multicast, and unknown unicast traffic streams.
- On EX9200 Ethernet Switches, Storm control is not enabled by default.
- On a QFX10002 switch, if storm control is configured on a VLAN port associated with an IRB interface, unregistered multicast traffic is classified as registered multicast traffic if IGMP snooping is enabled. If IGMP snooping is disabled, the traffic is classified as unknown unicast traffic.
- On switches other than QFX 10000 switches, storm control is applied in aggregate per port. That is, if you set a storm control level of 100 megabits and the sum of the broadcast, unknown unicast, and multicast traffic exceeds 100 megabits, storm control is initiated. On QFX 10000 switches, each traffic stream is measured independently per port, and storm control is initiated only if one of the streams exceeds the storm control level. For example, if you set a storm control level of 100 megabits and the broadcast and unknown unicast streams on the port are each flowing at 80 mbps, storm control is not triggered. In this case, storm control is initiated only if one of the streams exceeds 100 mbps.
- On QFX3500 series switches, when you configure storm control bandwidth, the value you configure is rounded off internally to the closest multiple of 64 Kbps, and the rounded-off value represents the bandwidth that is actually enforced. For example, if you configure a bandwidth limit of 150 Kbps, storm control enforces a bandwidth limit of 128 Kbps.
- Storm control is not enabled by default on Juniper Networks MX platforms.
- Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.
- In implementations of storm control prior to Junos version 17.3, rate limiting ingress traffic on a given port was based on PE trap-registers wherein the ingress traffic was rate limited per traffic type. As an example, in earlier implementations on applying a storm-control profile for BUM traffic at say x%; traffic would be rate limited per stream: broadcast, unknown unicast, multicast traffic individually to x% of link bandwidth. This behavior is different from rest of Junos implementation for storm-control where the net or aggregate traffic is rate limited to x% instead of per traffic type (broadcast, unknown unicast and multicast traffic). The implementation for Junos version 17.3 and later is based on policer resource per PE chip instead of the trap-registers and is coherent with the storm-control behavior across different Junos platforms.

Release History Table

Release	Description
17.4R1	Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.

Related Documentation

- [Enabling and Disabling Storm Control \(ELS\) on page 630](#)
- *action-shutdown*
- *port-error-disable*
- [storm-control on page 1016](#)

Enabling and Disabling Storm Control (non-ELS)



NOTE: If your switching device is an EX Series switch and runs Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, see [“Enabling and Disabling Storm Control \(ELS\)” on page 630](#).

The factory default configuration enables storm control on all EX Series switch interfaces, with the storm control level set to 80 percent of the combined applicable traffic streams, as follows:

- On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams.
- On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the combined broadcast, multicast, and unknown unicast streams.
- On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. Storm control can be disabled for each type of traffic individually.

You can disable storm control for all the applicable types of traffic on all interfaces or on a specified interface, as follows:

- On all switches—You can selectively disable storm control for broadcast streams, multicast streams, or for unknown unicast streams.
- On EX8200 switches—You can additionally selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic.
- On EX6200 switches—You can selectively disable storm control for each type of traffic individually.

You can enable storm control for multicast traffic (both registered and unregistered) on all interfaces or on a specific interface. This applies to all switches.

This topic describes:

- [Disabling Storm Control on Broadcast Traffic on page 628](#)
- [Disabling Storm Control on All Multicast Traffic on page 628](#)
- [Disabling Storm Control on Registered Multicast Traffic \(EX8200 Switches Only\) on page 628](#)
- [Disabling Storm Control on Unregistered Multicast Traffic \(EX8200 Switches Only\) on page 628](#)
- [Disabling Storm Control on Unknown Unicast Traffic on page 629](#)
- [Enabling Storm Control on Multicast Traffic on page 629](#)

Disabling Storm Control on Broadcast Traffic

To disable storm control on broadcast traffic:

- For all interfaces:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface all no-broadcast
```

- For an individual interface:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface interface-name no-broadcast
```

Disabling Storm Control on All Multicast Traffic

To disable storm control on all multicast traffic:

- For all interfaces:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface all no-multicast
```

- For an individual interface:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface interface-name no-multicast
```

Disabling Storm Control on Registered Multicast Traffic (EX8200 Switches Only)

To disable storm control only on registered multicast traffic (on EX8200 switches only):

- For all interfaces:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface all no-registered-multicast
```

- For an individual interface:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface interface-name no-registered-multicast
```

Disabling Storm Control on Unregistered Multicast Traffic (EX8200 Switches Only)

To disable storm control only on unregistered multicast traffic (on EX8200 switches only):

- For all interfaces:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface all no-unregistered-multicast
```

- For an individual interface:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface interface-name no-unregistered-multicast
```

Disabling Storm Control on Unknown Unicast Traffic

To disable storm control on unknown unicast traffic:

- For all interfaces:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface all no-unknown-unicast
```

- For an individual interface:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface interface-name no-unknown-unicast
```

Enabling Storm Control on Multicast Traffic

To enable storm control on multicast traffic:

- For all interfaces:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface all multicast
```

- For an individual interface:

```
[edit ethernet-switching-options]  
user@switch# set storm-control interface interface-name multicast
```

Related Documentation

- [Configuring Autorecovery for Port Security Events on page 635](#)
- [Understanding Storm Control on page 622](#)

Enabling and Disabling Storm Control (ELS)



NOTE: This task uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switching device is an EX Series switch and runs software that does not support ELS, see [“Understanding Storm Control” on page 622](#). If your switching device is an EX Series switch and runs software that does support ELS, see *Using the Enhanced Layer 2 Software CLI*.

On EX4300 switches, the factory default configuration enables storm control on all Layer 2 switch interfaces. The default storm control level is set to 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.

Storm control is not enabled by default on EX9200 switches or MX Series routers.

You can customize the storm control level for a specific interface. You specify the storm control level as the traffic rate in kilobits per second (Kbps) of the combined traffic streams or as the percentage of available bandwidth used by the combined traffic streams.

You can selectively disable storm control for broadcast, multicast, or unknown unicast traffic on all interfaces or on a specified interface. You can additionally disable storm control on registered or unregistered multicast traffic.

In the tasks described in this topic, you use the **[edit interfaces *interface-name* unit 0 family ethernet-switching]** hierarchy level to bind the storm control profile for EX Series switches and the **[edit interfaces *interface-name* unit 0 family bridge]** hierarchy level to bind the storm control profile for MX Series routers. Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.

- [Configuring Storm Control on page 631](#)
- [Disabling Storm Control on Broadcast Traffic on page 631](#)
- [Disabling Storm Control on All Multicast Traffic on page 632](#)
- [Disabling Storm Control on Registered Multicast Traffic on page 632](#)
- [Disabling Storm Control on Unregistered Multicast Traffic on page 633](#)
- [Disabling Storm Control on Unknown Unicast Traffic on page 633](#)
- [Disabling Storm Control on Multiple Types of Traffic on page 634](#)

Configuring Storm Control

You can configure storm control for a specific interface. The storm control level can be customized by explicitly configuring either the bandwidth level or the bandwidth percentage.

- **bandwidth-level**—Configures the storm control level as the bandwidth in kilobits per second of the combined traffic streams.
- **bandwidth-percentage**—Configures the storm control level as a percentage of the available bandwidth used by the combined traffic streams.

To configure storm control:

1. Create a storm control profile and set the storm control level as the traffic rate in kilobits per second of the combined traffic streams:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps
```



NOTE: The name of the storm control profile can contain no more than 127 characters.

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

Disabling Storm Control on Broadcast Traffic

To disable storm control on broadcast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams, and exclude broadcast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps no-broadcast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
```

```
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

Disabling Storm Control on All Multicast Traffic

To disable storm control on all multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams, but exclude multicast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps no-multicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

Disabling Storm Control on Registered Multicast Traffic

To disable storm control on only registered multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams, but exclude registered multicast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps no-registered-multicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

Disabling Storm Control on Unregistered Multicast Traffic

To disable storm control on only unregistered multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams, but exclude unregistered multicast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps
no-unregistered-multicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

Disabling Storm Control on Unknown Unicast Traffic

To disable storm control on only unknown unicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams, but exclude unregistered multicast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps
no-unknown-unicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

Disabling Storm Control on Multiple Types of Traffic

To disable storm control on multiple types of traffic; for example, broadcast and multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams but exclude broadcast and multicast traffic:

```
[edit forwarding-options]
user@device# set storm-control-profiles profile-name all bandwidth-level kbps no-broadcast
no-multicast
```

2. Bind the storm control profile to a logical interface:

For EX Series switches:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control
profile-name
```

For MX Series routers:

```
[edit]
user@device# set interfaces interface-name unit 0 family bridge storm-control profile-name
```

Release History Table

Release	Description
17.4R1	Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.

Related Documentation

- [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches](#)
- [Example: Using Storm Control to Prevent Network \(MX Routers\) on page 641](#)
- [Understanding Storm Control on page 622](#)

Configuring Autorecovery for Port Security Events

You can have the device automatically restore interfaces that have been disabled due to MAC limiting, MAC move limiting, or storm control conditions by configuring the **recovery-timeout** statement.

- To have EX series switches that support the Enhanced Layer 2 Software (ELS) configuration style automatically restore an interface that has been disabled due to MAC limiting, MAC move limiting, or storm control errors, set the following:

```
[edit interfaces interface-name unit 0 family bridge]
user@switch# set recovery-timeout 60
```

- To have MX routers or EX switches that do not support the Enhanced Layer 2 Software (ELS) configuration style automatically restore an interface that has been disabled due to MAC limiting, MAC move limiting, or storm control errors, set the following:

```
[edit ethernet-switching-options interface-name unit 0 family bridge]
user@switch# set recovery-timeout 60
```

An interface may shut down or be disabled as a result of one of the following port-security or storm-control configurations:

- Storm control—The **storm-control** statement is configured with the **action-shutdown** statement, or the action **shutdown**, depending on the platform you are using.
- MAC limiting—(Not supported on MX Series routers) The **mac-limit** statement is configured with the **action-shutdown** statement, or the action **shutdown**, depending on the platform you are using.
- MAC move limiting—(Not supported on MX Series routers) The **mac-move-limit** statement is configured with the **action-shutdown** statement, or the action **shutdown**, depending on the platform you are using.

There is no default, so unless the statement is explicitly configured, you will need to manually restore the interfaces by running a clear command.

- For EX Series switches, run: **clear ethernet-switching recovery-timeout**
- For MX Series routers, run: **clear bridge recovery-timeout**

Related Documentation

- For ELS details, see *Using the Enhanced Layer 2 Software CLI*
- *Configuring MAC Limiting (ELS)*
- *Configuring MAC Move Limiting (ELS)* on page 365
- *Enabling and Disabling Storm Control (ELS)* on page 630

Example: Using Storm Control to Prevent Network Outages

Using storm control can prevent problems caused by broadcast storms. You can configure storm control to rate-limit broadcast traffic, multicast traffic (on some devices), and unknown unicast traffic at a specified level so that the switch drops packets when the specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. You can also have the device shut down or temporarily disable an interface when the storm control limit is exceeded.

A traffic storm occurs when broadcast packets prompt receiving devices to broadcast packets in response. This prompts further responses, creating a knock-on effect that results in a broadcast storm that floods the device with packets, and causing poor performance or even a complete loss of service by some clients

Storm control monitors the level of applicable incoming traffic and compares it with the level that you specify. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. As an alternative to having the switch drop packets, you can configure storm control to shut down interfaces or temporarily disable interfaces (see the [action-shutdown](#) statement or the [recovery-timeout](#) statement) when the storm control level is exceeded.

- On ELS systems, storm control is enabled by default on all interfaces at a level of 80 percent of the available bandwidth.
- On non-ELS systems, storm control is disabled by default on all interfaces. If you enable storm control, the default level is 80 percent of the available bandwidth.



NOTE: If you configure storm control on an aggregated Ethernet interface, the storm-control level is applied to each member interface individually. For example, if the aggregated interface has two members and you configure a storm-control level of 20 kbps, Junos will not detect a storm if one or both of the member interfaces receives traffic at 15 kbps because in neither of these cases does an individual member receive traffic at a rate greater than the configured storm-control level. In this example, Junos detects a storm only if at least one member interface receives traffic at greater than 20 Kbps.

- On EX2200, EX3200, EX3300, and EX4200 switches—Storm control is not enabled for multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams.
- On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.
- On EX6200 switches—Storm control is not enabled for multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent

of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. Storm control can be disabled for each type of traffic individually.

- [Example: Using Storm Control to Prevent Network Outages \(ELS\) on page 637](#)
- [Example: Using Storm Control to Prevent Network Outages \(non-ELS\) on page 638](#)
- [Example: Using Storm Control to Prevent Network \(MX Routers\) on page 641](#)

Example: Using Storm Control to Prevent Network Outages (ELS)

This example uses a Junos OS release that supports the Enhanced Layer 2 Software (ELS) configuration style.

- [Requirements on page 637](#)
- [Overview and Topology on page 637](#)
- [Configuration on page 637](#)

Requirements

This example uses the following hardware and software components:

- One QFX Series switch running Junos OS with ELS
- Junos OS Release 13.2 or later

Overview and Topology



NOTE:

The topology used in this example consists of one switch connected to various network devices. This example shows how to configure the storm control level on interface xe-0/0/0 by setting the level to a traffic rate of 15,000 Kbps, based on the traffic rate of the combined applicable traffic streams. If the combined traffic exceeds this level, the switch drops packets for the controlled traffic types to prevent a network outage.

Configuration

CLI Quick Configuration

To quickly configure storm control based on the traffic rate in kilobits per second of the combined traffic streams, copy the following command and paste it into the switch terminal window:

```
[edit]
set forwarding-options storm-control-profiles sc-profile all bandwidth-level 15000
set interfaces xe-0/0/0 unit 0 family ethernet-switching storm-control sc-profile
```

Step-by-Step Procedure

To configure storm control:

1. Configure a storm control profile, **sc-profile**, and specify the traffic rate in kilobits per second of the combined traffic streams:

```
[edit]
user@switch> set forwarding-options storm-control-profiles sc-profile all bandwidth-level
15000
```

2. Bind the storm control profile, **sc**, to a logical interface:

```
[edit]
user@switch> set interfaces xe-0/0/0 unit 0 family ethernet-switching storm-control
sc-profile
```

Results Display the results of the configuration:

```
[edit forwarding-options]
user@switch> show storm-control-profiles sc-profile
all {
    bandwidth 15000;
}
```

```
[edit]
user@switch> show interfaces xe-0/0/0
unit 0 {
    family ethernet-switching {
        vlan {
            members default;
        }
        storm-control sc-profile;
    }
}
```

- See Also**
- [Understanding Storm Control on page 622](#)
 - [Example: Using Storm Control to Prevent Network Outages on page 636](#)

Example: Using Storm Control to Prevent Network Outages (non-ELS)

This example uses a Junos OS release that does not support the Enhanced Layer 2 Software (ELS) configuration style on a single EX Series switch. If your switch runs software that supports ELS, see [“Example: Using Storm Control to Prevent Network Outages \(ELS\)” on page 637](#). For information about how to configure the switch to shut down or temporarily disable an interface when the storm control limit is exceeded, see [“Example: Using Storm Control to Prevent Network Outages” on page 636](#)

- [Requirements on page 639](#)
- [Overview and Topology on page 639](#)
- [Configuration on page 639](#)
- [Verification on page 639](#)

Requirements

This example uses the following hardware and software components:

- A switch
- Junos OS Release 11.1 or later

Overview and Topology

This example shows how to configure the storm control level on interface **xe-0/0/0** by setting the level to a traffic rate of 5000000 Kbps, based on the total of the combined broadcast and unknown unicast streams. If broadcast traffic and unknown unicast traffic exceed these levels, the switch drops packets for the controlled traffic types.

Configuration

Step-by-Step Procedure

To configure storm control for a 10-Gigabit Ethernet interface to the equivalent of 50 percent of the available bandwidth:

- Specify the level of allowed broadcast traffic and unknown unicast traffic on a specific interface:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface xe-0/0/0 bandwidth 5000000
```

Results Display the results of the configuration:

```
[edit ethernet-switching-options]
user@switch# show storm-control
interface xe-0/0/0 {
    bandwidth 5000000;
}
```

Verification

Verifying That the Storm Control Configuration Is in Effect

Purpose Confirm that storm control is limiting the rate of traffic on the interface.

Action Use the **show interfaces ge-0/0/0 detail** or **show interfaces ge-0/0/0 extensive** operational mode command to view traffic statistics on the storm controlled interface. The input rate (bps) must not exceed the storm control limit.

```
user@switch> show interfaces ge-0/0/0 extensive
Physical interface: ge-0/0/0, Enabled, Physical link is Up
Interface index: 160, SNMP ifIndex: 503, Generation: 163
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto,
BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
```

```

Remote fault: Online
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: b0:c6:9a:67:90:84, Hardware address: b0:c6:9a:67:90:84
Last flapped : 2013-05-16 22:46:42 UTC (14w3d 03:13 ago)
Statistics last cleared: Never
Traffic statistics: 5000000
Input bytes : 312742788 512 bps
Output bytes : 245552919 0 bps
Input packets: 3550009 1 pps
Output packets: 2622101 0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Dropped traffic statistics due to STP State:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runt: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets:
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets

0 best-effort 0 1 0
1 assured-forw 0 0 0
5 expedited-fo 0 0 0
7 network-cont 0 2622100 0

Queue number: Mapped forwarding classes
0 best-effort
1 assured-forwarding
5 expedited-forwarding
7 network-control

Active alarms : None
Active defects : None
MAC statistics:

```

	Receive	Transmit
Total octets	0	0
Total packets	0	0
Unicast packets	0	0
Broadcast packets	0	0
Multicast packets	0	0
CRC/Align errors	0	0
FIFO errors	0	0
MAC control frames	0	0
MAC pause frames	0	0
Oversized frames	0	0

```

Jabber frames                0
Fragment frames              0
VLAN tagged frames           0
Code violations               0
Autonegotiation information:
  Negotiation status: Incomplete
Packet Forwarding Engine configuration:
  Destination slot: 0
Interface transmit statistics: Disabled

```

Meaning The traffic statistics **input bytes field** shows the ingress traffic rate at 512 bits per second (bps). This rate is within the storm control limit of 5000000 Kbps.

- See Also**
- [Understanding Storm Control on page 622](#)
 - [Enabling and Disabling Storm Control \(non-ELS\) on page 626](#)
 - *action-shutdown*
 - *interface (Storm Control)*
 - *port-error-disable*

Example: Using Storm Control to Prevent Network (MX Routers)

This example shows how to configure storm control on an pair of MX Series routers running Junos OS with Enhanced Layer 2 Software (ELS).

- [Requirements on page 641](#)
- [Overview and Topology on page 641](#)
- [Configuration on page 642](#)
- [Verification on page 644](#)

Requirements

This example uses the following hardware and software components:

- Two MX Series routers
- Junos OS Release 14.1 or later with ELS
- A traffic generator that can send broadcast and unknown unicast traffic at a rate that exceeds 100 Kbps
- A second host

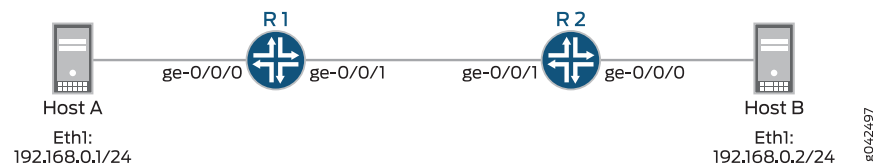
Overview and Topology

On MX Series routers, storm control is not enabled by default.

This example shows how to configure the storm control level on interface ge-0/0/1 by setting the level to a traffic rate of 100 Kbps. The topology used consists of two routers

that could be connected to various network devices. If the combined traffic exceeds this level, the router drops packets for the controlled traffic types to prevent a network outage. (Starting in Junos OS release 17.4R1 for MX Series routers, you can also configure storm control on logical systems.)

Figure 43: Example Storm Control to Prevent Network Outages



Configuration

This example excludes multicast traffic from the storm traffic. Many protocols use multicast for control traffic, and for that reason network administrators and operators may want to keep multicast working to avoid obstructing protocol operation.

CLI Quick Configuration

To quickly configure storm control based on the traffic rate in Kbps of the combined traffic streams, copy the following commands and paste them into the terminal window. The configurations of routers R1 and R2 are exactly the same:

```

set interfaces ge-0/0/0 unit 0 family bridge interface-mode access
set interfaces ge-0/0/0 unit 0 family bridge vlan-id 15
set interfaces ge-0/0/1 vlan-tagging
set interfaces ge-0/0/1 unit 0 family bridge interface-mode trunk
set interfaces ge-0/0/1 unit 0 family bridge vlan-id-list 15
set interfaces ge-0/0/1 unit 0 family bridge storm-control sc
set interfaces ge-0/0/1 unit 0 family bridge recovery-timeout 120
set bridge-domains bd1 domain-type bridge vlan-id 15
set forwarding-options storm-control-profiles sc all bandwidth-level 100 no multicast
set forwarding-options storm-control-profiles sc action-shutdown
  
```

Step-by-Step Procedure

To configure storm control:

1. Configure a storm control profile, **sc**, and specify the traffic rate in Kbps of the combined traffic streams. Exclude multicast traffic from the storm control profile.

```

[edit]
user@host# set forwarding-options storm-control-profiles sc all bandwidth-level 100 no-multicast
user@host# set forwarding-options storm-control-profiles sc action-shutdown
  
```

2. Bind the storm control profile **sc** to a logical interface. Remember to do this for both interfaces between the routers.

```

[edit]
user@host# set interfaces ge-0/0/1 unit 0 family bridge storm-control sc
  
```

3. Configure interface ge-0/0/1 (the interface between routers). Do this for both interfaces between the routers.

```
[edit]
user@host# set interfaces ge-0/0/1 vlan-tagging
user@host# set interfaces ge-0/0/1 unit 0 family bridge interface-mode trunk
user@host# set interfaces ge-0/0/1 unit 0 family bridge vlan-id-list 15
user@host# set interfaces ge-0/0/1 unit 0 family bridge recovery-timeout 120
```

4. Configure interface ge-0/0/0 (the interface from host to router). Remember to do this for both interfaces between the routers.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family bridge interface-mode access
user@host# set interfaces ge-0/0/0 unit 0 family bridge vlan-id 15
```

5. Set the bridge domain domain type and VLAN ID.

```
[edit]
user@host# set bridge-domains bd1 domain-type bridge vlan-id 15
```

Results Display the results of the configuration:

```
[edit forwarding-options]
user@router> show storm-control-profiles sc
all {
  bandwidth-level 100;
  no-multicast;
}
action-shutdown;
```

```
[edit]
user@router> show interfaces ge-0/0/0
unit 0 {
  family bridge {
    interface-mode access;
    vlan-id 15;
  }
}
```

```
[edit]
user@router> show interfaces ge-0/0/1
vlan-tagging;
unit 0 {
  family bridge {
    interface-mode trunk;
    vlan-id-list 15;
    storm-control sc;
    recovery-timeout 120;
```

```
}
}
```

```
[edit]
user@router> show bridge-domains bd1
domain-type bridge;
vlan-id 15;
```

Verification

Verifying That the Storm Control Configuration Is in Effect

Purpose Confirm that storm control is limiting the rate of traffic on the interface.

- Action**
1. From Host A to Host B, use a traffic generator to send broadcast and unknown unicast traffic at a rate that exceeds 100 Kbps.
 2. Verify on device R1's ge-0/0/0 interface that traffic is entering at a rate that exceeds 100 Kbps.

```
user@R1# run show interfaces detail ge-0/0/0
```

```
Physical interface: ge-0/0/0, Enabled, Physical link is Up
Interface index: 137, SNMP ifIndex: 513, Generation: 140
Link-level type: Ethernet-Bridge, MTU: 1514, MRU: 1522, Speed: 1000mbps,
BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Pad to minimum frame size: Disabled
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x20004000
Link flags     : None
CoS queues    : 8 supported, 8 maximum usable queues
Hold-times    : Up 0 ms, Down 0 ms
Current address: 00:05:86:71:6a:00, Hardware address: 00:05:86:71:6a:00
Last flapped   : 2014-05-20 14:43:25 PDT (1w1d 01:20 ago)
Statistics last cleared: 2014-05-28 15:59:39 PDT (00:04:02 ago)
Traffic statistics:
Input bytes   :          830088          180432 bps
Output bytes  :           0          0 bps
Input packets :          8472          230 pps
Output packets:           0          0 pps
IPv6 transit statistics:
Input bytes   :           0
Output bytes  :           0
Input packets :           0
Output packets:           0
Active alarms : None
Active defects: None
Interface transmit statistics: Disabled
```

The Input bytes field shows the ingress traffic rate in bytes per second (bps). The input rate is within the storm control limit of 100 Kbps.

3. Verify that interface ge-0/0/1 on R1 is down (Admin down).


```
user@R1# run show interfaces ge-0/0/1.0 terse
```

Interface	Admin	Link	Proto	Local	Remote
ge-0/0/1.0	down	up	bridge		

Because the link remains up, control traffic continues to flow.

4. After the timeout period of 120 seconds (2 minutes), verify that the interface comes back up.

```
user@R1# run show interfaces ge-0/0/1.0 terse
```

Interface	Admin	Link	Proto	Local	Remote
ge-0/0/1.0	up	up	bridge		

- See Also**
- [Enabling and Disabling Storm Control \(ELS\) on page 630](#)
 - [Configuring Autorecovery for Port Security Events on page 635](#)

PART 13

Configuration Statements and Operational Commands

- Configuration Statements on page 649
- Operational Commands on page 1067

CHAPTER 27

Configuration Statements

- Security Services Configuration Statements on page 658
- accept on page 660
- accept-source-mac on page 662
- access-security on page 664
- action-priority on page 666
- action-shutdown on page 667
- algorithm (Authentication Keychain) on page 669
- algorithm (Junos FIPS) on page 669
- allowed-mac on page 670
- arp-inspection on page 671
- arp-inspection (MX Series) on page 672
- authentication (Security IPsec) on page 673
- authentication-algorithm (Security IKE) on page 674
- authentication-algorithm (Security IPsec) on page 675
- authentication-key-chains on page 677
- authentication-method on page 678
- auto-re-enrollment on page 679
- auxiliary-spi (Security IPsec) on page 680
- bandwidth on page 681
- bandwidth (DDoS) on page 682
- bandwidth-level on page 683
- bandwidth-percentage on page 685
- bandwidth-scale (DDoS) on page 686
- bridge-domains on page 687
- burst (DDoS) on page 688
- burst-scale (DDoS) on page 689
- bypass-aggregate (DDoS) on page 690
- cache-size on page 691

- [cache-timeout-negative](#) on page 692
- [ca-identity](#) on page 693
- [cak](#) on page 694
- [cak \(MX Series\)](#) on page 695
- [ca-name](#) on page 696
- [ca-profile \(Security PKI\)](#) on page 697
- [certificate-id](#) on page 698
- [certificates](#) on page 699
- [certification-authority](#) on page 700
- [challenge-password](#) on page 701
- [children](#) on page 702
- [cipher-suite \(MACsec\)](#) on page 704
- [circuit-id](#) on page 706
- [ckn](#) on page 707
- [connections \(Host VPN\)](#) on page 708
- [connectivity-association](#) on page 710
- [connectivity-association \(MACsec Interfaces\)](#) on page 711
- [connectivity-association \(MACsec Interfaces for MX Series\)](#) on page 712
- [crl \(Adaptive Services Interface\)](#) on page 713
- [crl \(Encryption Interface\)](#) on page 714
- [ddos-protection \(DDoS\)](#) on page 715
- [description \(Authentication Keychain\)](#) on page 718
- [description \(IKE policy\)](#) on page 719
- [dhcp-option82](#) on page 720
- [dhcp-security](#) on page 721
- [dhcp-security \(MX Series\)](#) on page 724
- [dhcp-service](#) on page 726
- [dhcp-snooping-file](#) on page 728
- [dhcp-snooping-file](#) on page 729
- [dhcp-trusted](#) on page 730
- [dhcpv6-options](#) on page 731
- [dhcpv6-snooping-file](#) on page 732
- [dh-group](#) on page 733
- [direction](#) on page 734
- [direction \(Junos OS\)](#) on page 735
- [direction \(Junos-FIPS Software\)](#) on page 736
- [direction \(MX Series\)](#) on page 737

- [disable-fpc \(DDoS\) on page 738](#)
- [disable-logging \(DDoS\) on page 739](#)
- [disable-preceding-key on page 740](#)
- [disable-routing-engine \(DDoS\) on page 741](#)
- [disable-timeout on page 742](#)
- [disable-timeout \(Port Error Disable\) on page 743](#)
- [discard on page 744](#)
- [dynamic on page 745](#)
- [encoding on page 746](#)
- [encryption \(MACsec\) on page 747](#)
- [encryption \(MACsec for MX Series\) on page 748](#)
- [encryption \(Junos OS\) on page 749](#)
- [encryption \(Junos-FIPS Software\) on page 750](#)
- [encryption-algorithm \(Security\) on page 751](#)
- [enrollment on page 752](#)
- [enrollment-retry on page 753](#)
- [enrollment-url on page 754](#)
- [ethernet-switching-options on page 755](#)
- [examine-dhcp on page 761](#)
- [examine-dhcpv6 on page 763](#)
- [examine-fip on page 765](#)
- [exclude-protocol on page 766](#)
- [exclude-protocol \(MX Series\) on page 767](#)
- [fallback-key on page 768](#)
- [family vpls \(Layer 2 Pseudowires\) on page 769](#)
- [fc-map on page 770](#)
- [fcoe-trusted on page 772](#)
- [file on page 773](#)
- [flood \(VLANs\) on page 774](#)
- [flow-detection \(DDoS Flow Detection\) on page 775](#)
- [flow-detection \(DDoS Packet Level\) on page 776](#)
- [flow-detection-mode \(DDoS Flow Detection\) on page 777](#)
- [flow-detection-mode \(DDoS Global Flow Detection\) on page 778](#)
- [flow-detect-time \(DDoS Flow Detection\) on page 779](#)
- [flow-level-bandwidth \(DDoS Flow Detection\) on page 780](#)
- [flow-level-control \(DDoS Flow Detection\) on page 781](#)
- [flow-level-control \(DDoS Global Flow Detection\) on page 782](#)

- [flow-level-detection \(DDoS Flow Detection\)](#) on page 783
- [flow-recover-time \(DDoS Flow Detection\)](#) on page 784
- [flow-report-rate \(DDoS Flow Detection\)](#) on page 785
- [flow-timeout-time \(DDoS Flow Detection\)](#) on page 786
- [forwarding-class \(for DHCP Snooping or DAI Packets\)](#) on page 787
- [forwarding-options](#) on page 788
- [fpc \(DDoS\)](#) on page 794
- [global \(DDoS\)](#) on page 795
- [group \(DHCP Security\)](#) on page 796
- [group \(DHCP Security for MX Series\)](#) on page 797
- [group-type \(Unknown Unicast Forwarding\)](#) on page 798
- [host-name](#) on page 799
- [host-vpn](#) on page 800
- [id](#) on page 801
- [id \(MACsec for MX Series\)](#) on page 802
- [identity](#) on page 802
- [ike \(Security\)](#) on page 803
- [ike-log](#) on page 804
- [ike-secrets](#) on page 805
- [include-sci](#) on page 806
- [include-sci \(MACsec for MX Series\)](#) on page 807
- [interface \(Access Port Security\)](#) on page 808
- [interface \(DHCP Security for MX Series\)](#) on page 809
- [interface \(RA Guard\)](#) on page 810
- [interface \(Secure Access Port\)](#) on page 811
- [interface \(Static MAC Bypass\)](#) on page 812
- [interface \(Storm Control\)](#) on page 813
- [interface \(Unknown Unicast Forwarding\)](#) on page 814
- [interface-mac-limit](#) on page 815
- [interface-shutdown-action](#) on page 817
- [interfaces \(MACsec\)](#) on page 818
- [interfaces \(MACsec for MX Series\)](#) on page 819
- [internal](#) on page 820
- [ipsec \(Security\)](#) on page 821
- [ip-source-guard](#) on page 823
- [ip-source-guard \(MX Series\)](#) on page 825
- [source-ip-address-list](#) on page 826

- [ipv6-source-guard](#) on page 827
- [ipv6-source-guard-sessions](#) on page 828
- [key \(Authentication Keychain\)](#) on page 829
- [key \(Junos FIPS\)](#) on page 830
- [key \(MACsec\)](#) on page 831
- [key-chain \(Security\)](#) on page 832
- [key-server-priority \(MACsec\)](#) on page 833
- [key-server-priority \(MACsec for MX Series\)](#) on page 834
- [ldap-url](#) on page 835
- [level](#) on page 836
- [lifetime-seconds \(Security\)](#) on page 837
- [light-weight-dhcpv6-relay](#) on page 838
- [local](#) on page 840
- [local-certificate \(Security\)](#) on page 841
- [local-key-pair](#) on page 841
- [local-traffic-selector](#) on page 842
- [location](#) on page 843
- [location \(DHCP Snooping Database\)](#) on page 844
- [logical-interface \(DDoS Flow Detection\)](#) on page 845
- [mac](#) on page 847
- [mac \(Option 82\)](#) on page 848
- [mac-address \(MACsec\)](#) on page 849
- [mac-address \(MACsec\)](#) on page 850
- [mac-limit](#) on page 851
- [mac-limit \(Access Port Security\)](#) on page 852
- [mac-list](#) on page 853
- [mac-move-limit](#) on page 854
- [macsec](#) on page 856
- [macsec \(MX Series\)](#) on page 858
- [manual \(Junos OS\)](#) on page 859
- [manual \(Junos-FIPS Software\)](#) on page 860
- [mark-interface \(RA Guard\)](#) on page 861
- [match-list](#) on page 862
- [match-option](#) on page 864
- [maximum-certificates](#) on page 865
- [mka](#) on page 866
- [mka \(MX Series\)](#) on page 867

- [mode \(IKE\) on page 868](#)
- [mode \(IPsec\) on page 869](#)
- [multicast on page 870](#)
- [must-secure on page 871](#)
- [neighbor-discovery-inspection on page 872](#)
- [next-hop-group \(Unknown Unicast Forwarding\) on page 873](#)
- [no-allowed-mac-log on page 874](#)
- [no-broadcast on page 875](#)
- [no-dhcp-snooping on page 877](#)
- [no-dhcp-trusted on page 878](#)
- [no-dhcpv6-options on page 879](#)
- [no-dhcpv6-snooping on page 879](#)
- [no-encryption \(MACsec\) on page 880](#)
- [no-encryption \(MACsec for MX Series\) on page 881](#)
- [no-examine-dhcpv6 on page 882](#)
- [no-fcoe-trusted on page 883](#)
- [no-flow-logging \(DDoS Flow Detection\) on page 884](#)
- [no-gratuitous-arp-request on page 885](#)
- [no-gratuitous-arp-request on page 886](#)
- [no-multicast on page 887](#)
- [no-option16 on page 888](#)
- [no-option18 on page 889](#)
- [no-option37 on page 889](#)
- [no-option82 on page 890](#)
- [no-registered-multicast on page 891](#)
- [no-unknown-unicast on page 892](#)
- [no-unregistered-multicast on page 894](#)
- [offset on page 895](#)
- [offset \(MX Series\) on page 897](#)
- [option-16 \(DHCPv6 Snooping\) on page 898](#)
- [option-18 \(DHCPv6 Snooping\) on page 899](#)
- [option-37 \(DHCPv6 Snooping\) on page 901](#)
- [no-option-37 on page 902](#)
- [option-82 on page 903](#)
- [options \(Security\) on page 904](#)
- [overrides \(DHCP Security\) on page 905](#)
- [overrides \(DHCP Security for MX Series\) on page 906](#)

- [packet-action](#) on page 907
- [path-length](#) on page 910
- [perfect-forward-secrecy \(Security\)](#) on page 911
- [perfect-forward-secrecy \(Services\)](#) on page 912
- [persistent-learning](#) on page 913
- [persistent-learning](#) on page 914
- [physical-interface \(DDoS Flow Detection\)](#) on page 915
- [pki](#) on page 917
- [policy](#) on page 919
- [policy \(Security IKE\)](#) on page 920
- [policy \(Security IPsec\)](#) on page 921
- [port-error-disable](#) on page 922
- [port-id](#) on page 923
- [port-id \(MACsec for MX Series\)](#) on page 924
- [prefix \(Circuit ID for Option 82\)](#) on page 925
- [prefix \(DHCPv6 Options\)](#) on page 927
- [prefix \(Remote ID for Option 82\)](#) on page 928
- [prefix-list-name](#) on page 929
- [pre-shared-key](#) on page 930
- [pre-shared-key \(MX Series\)](#) on page 931
- [pre-shared-key \(Security\)](#) on page 932
- [priority \(DDoS\)](#) on page 933
- [proposal \(Security IKE\)](#) on page 934
- [proposal \(Security IPsec\)](#) on page 935
- [proposals](#) on page 936
- [protocol \(Junos OS\)](#) on page 937
- [protocol \(Junos-FIPS Software\)](#) on page 938
- [protocols \(DDoS\)](#) on page 939
- [protocols \(DDoS\) \(PTX Series and QFX Series\)](#) on page 950
- [recover-time \(DDoS\)](#) on page 958
- [recovery-timeout](#) on page 959
- [re-enroll-trigger-time-percentage](#) on page 960
- [refresh-interval](#) on page 961
- [re-generate-keypair](#) on page 961
- [remote \(Host VPN\)](#) on page 962
- [remote-id](#) on page 963
- [remote-id \(MX Series\)](#) on page 965

- [replay-protect](#) on page 966
- [replay-protect \(MX Series\)](#) on page 967
- [remote-traffic-selector](#) on page 968
- [replay-window-size \(MX Series\)](#) on page 969
- [replay-window-size](#) on page 970
- [retry \(Adaptive Services Interface\)](#) on page 971
- [retry-interval](#) on page 972
- [revocation-check](#) on page 973
- [router-advertisement-guard](#) on page 974
- [routing-instance-name](#) on page 976
- [routing-instance-name \(circuit-id\)](#) on page 976
- [rpf-check](#) on page 977
- [secret](#) on page 978
- [secure-access-port](#) on page 979
- [secure-channel](#) on page 981
- [secure-channel](#) on page 982
- [security](#) on page 983
- [security-association](#) on page 985
- [security-association \(Junos OS\)](#) on page 986
- [security-association \(Junos-FIPS Software\)](#) on page 987
- [security-mode](#) on page 988
- [show ddos-protection protocols culprit-flows](#)
- [show ddos-protection protocols flow-detection](#)
- [source-mac-address-list](#) on page 1001
- [spi \(Junos OS\)](#) on page 1002
- [spi \(Junos-FIPS Software\)](#) on page 1003
- [ssh](#) on page 1004
- [ssh-known-hosts](#) on page 1006
- [start-time \(Authentication Key Transmission\)](#) on page 1008
- [stateful](#) on page 1010
- [stateless](#) on page 1011
- [static-ip](#) on page 1012
- [static-ip \(MX Series\)](#) on page 1013
- [static-ipv6](#) on page 1014
- [storm-control](#) on page 1015
- [storm-control](#) on page 1016
- [storm-control](#) on page 1017

- [storm-control-profiles](#) on page 1018
- [subscriber](#) (DDoS Flow Detection) on page 1019
- [switch-options](#) (VLANs) on page 1021
- [timeout](#) on page 1023
- [timeout-active-flows](#) (DDoS Flow Detection) on page 1024
- [tolerance](#) on page 1025
- [traceoptions](#) on page 1026
- [traceoptions](#) (Access Port Security) on page 1028
- [traceoptions](#) (DDoS) on page 1031
- [traceoptions](#) (DHCP) on page 1033
- [traceoptions](#) (MACsec) on page 1036
- [traceoptions](#) (MACsec interfaces) on page 1038
- [transmit-interval](#) (MACsec) on page 1040
- [transmit-interval](#) (MACsec for MX Series) on page 1041
- [trusted](#) on page 1042
- [trusted](#) (DHCP Security) on page 1042
- [unknown-unicast-forwarding](#) on page 1043
- [untrusted](#) on page 1044
- [untrusted](#) on page 1045
- [url](#) (Security) on page 1046
- [use-interface-description](#) on page 1047
- [use-interface-description](#) on page 1049
- [use-interface-index](#) on page 1051
- [use-interface-name](#) on page 1052
- [use-string](#) on page 1053
- [use-vlan-id](#) on page 1054
- [validity-period](#) on page 1055
- [vendor-id](#) on page 1056
- [violation-report-rate](#) (DDoS Flow Detection) on page 1057
- [vlan](#) (Access Port Security) on page 1058
- [vlan](#) (DHCP Bindings on Access Ports) on page 1060
- [vlans](#) (RA Guard) on page 1061
- [vlan](#) (Secure Access Port) on page 1062
- [vlan](#) (Static IP) on page 1063
- [vlan](#) (Unknown Unicast Forwarding) on page 1064
- [voip-mac-exclusive](#) on page 1065
- [write-interval](#) on page 1066

Security Services Configuration Statements

The following table lists the security services configuration statements available at the **[edit security]** hierarchy level:

Table 34: Security Services Configuration Statements

A-C	D-G	H-M	N-R	S-Z
algorithm (Authentication Keychain)	description (Authentication Keychain)	identity	options (Security)	secret
algorithm (Junos FIPS)	description (IKE policy)	ike	path-length	security-association (Junos OS)
authentication (Security IPsec)	dh-group	internal	perfect-forward-secrecy (Security)	security-association (Junos-FIPS Software)
authentication-algorithm (Security IKE)	direction (Junos OS)	ipsec (Security)	pki	spi (Junos OS)
authentication-algorithm (Security IPsec)	direction (Junos-FIPS Software)	key (Authentication Keychain)	policy (Security IKE)	spi (Junos-FIPS Software)
authentication-key-chains	dynamic	key (Junos FIPS)	policy (Security IPsec)	ssh-known-hosts
authentication-method	encoding	key-chain (Security)	pre-shared-key (Security)	start-time (Authentication Key Transmission)
auto-re-enrollment	encryption (Junos OS)	ldap-url	proposal (Security IKE)	tolerance
auxiliary-spi	encryption (Junos-FIPS Software)	lifetime-seconds (Security)	proposal (Security IPsec)	traceoptions
ca-identity	encryption-algorithm	local	proposals	url
ca-name	enrollment	local-certificate (Security)	protocol (Junos OS)	validity-period
ca-profile	enrollment-retry	local-key-pair	protocol (Junos-FIPS Software)	
cache-size	enrollment-url	manual (Junos OS)	re-enroll-trigger-time-percentage	
cache-timeout-negative	file	manual (Junos-FIPS Software)	re-generate-keypair	
certificate-id		maximum-certificates	refresh-interval	
certificates		mode (IKE)	retry (Adaptive Services Interface)	

Table 34: Security Services Configuration Statements (continued)

A-C	D-G	H-M	N-R	S-Z
certification-authority		mode (IPsec)	retry-interval	
challenge-password			revocation-check	
crl (Adaptive Services Interface)				
crl (Encryption Interface)				

Related Documentation • [\[edit security\] Hierarchy Level](#)

accept

Syntax

```
accept {
  match-list {
    match-criteria {
      (match-all | match-any);
    }
    prefix-list-name prefix-list-name;
    source-ip-address-list address-list-name;
    source-mac-address-list address-list-name;
  }
  match-option {
    hop-limit {
      (maximum | minimum) value;
    }
    managed-config-flag;
    other-config-flag;
    router-preference (high | low | medium);
  }
}
```

Hierarchy Level [edit forwarding-options access-security [router-advertisement-guard policy](#) *policy-name*]

Release Information Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.
Statement introduced in Junos OS Release 16.1 for EX Series switches.

Description Configure the accept policy for an IPv6 Router Advertisement (RA) guard policy. RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in the policy.

When RA guard is enabled, the switch compares the information contained in the attributes of RA messages to the information contained in the policy. If RA guard is enabled by using an accept policy, any RA messages that match the conditions defined in the policy are forwarded, and RA messages that do not match the conditions are dropped.

The criteria are configured either as one or more lists of source address or address prefixes, which are associated with the accept policy by using the [match-list](#) statement, or match condition parameters, which are associated with the accept policy by using the [match-option](#) statement.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring Stateless IPv6 Router Advertisement Guard on page 517](#)
 - [Configuring Stateful IPv6 Router Advertisement Guard on page 514](#)

accept-source-mac

Syntax	<pre>accept-source-mac { mac-address <i>mac-address</i> { policer { input <i>cos-policer-name</i>; output <i>cos-policer-name</i>; } } }</pre>
Hierarchy Level	<pre>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</pre>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 12.1X48 for PTX Packet Transport Routers.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p>
Description	<p>For Gigabit Ethernet intelligent queuing (IQ) interfaces only, accept traffic from and to the specified remote media access control (MAC) address.</p> <p>The accept-source-mac statement is equivalent to the source-address-filter statement, which is valid for aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only. To allow the interface to receive packets from specific MAC addresses, include the accept-source-mac statement.</p> <p>On untagged Gigabit Ethernet interfaces, you should not configure the source-address-filter statement and the accept-source-mac statement simultaneously. On tagged Gigabit Ethernet interfaces, you should not configure the source-address-filter statement and the accept-source-mac statement with an identical MAC address specified in both filters.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>



NOTE: The **policer** statement is not supported on PTX Series Packet Transport Routers.



NOTE: On QFX platforms, if you configure source MAC addresses for an interface using the *static-mac* or **persistent-learning** statements and later configure a different MAC address for the same interface using the **accept-source-mac** statement, the MAC addresses that you previously configured for the interface remain in the ethernet-switching table and can still be used to send packets to the interface.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring MAC Address Filtering</i>• <i>Configuring MAC Address Filtering on PTX Series Packet Transport Routers</i>• <i>source-filtering</i>

access-security

```
Syntax access-security {
  router-advertisement-guard {
    interface interface-name {
      mark-interface (trusted | block);
      policy policy-name (stateful | stateless);
    }
    vlans (vlan-name | all) {
      policy policy-name (stateful | stateless);
    }
    policy policy-name {
      accept {
        match-list {
          match-criteria {
            (match-all | match-any);
          }
          prefix-list-name prefix-list-name;
          source-ip-address-list address-list-name;
          source-mac-address-list address-list-name;
        }
        match-option {
          hop-limit {
            (maximum | minimum) value;
          }
          managed-config-flag;
          other-config-flag;
          router-preference (high | low | medium);
        }
      }
      discard {
        prefix-list-name prefix-list-name;
        source-ip-address-list address-list-name;
        source-mac-address-list address-list-name;
      }
    }
  }
  slaac-snooping {
    interface (interface-name | all) {
      auto-dad {
        retries retries;
        retrans-interval seconds;
      }
      mark-interface {
        trusted;
      }
      max-allowed-contentions count {
        duration seconds;
      }
    }
    link-local {
      expiry interval seconds;
    }
  }
}
```

```

    vlans (vlan-name | all);
  }
}

```

Hierarchy Level [edit forwarding-options]

Release Information Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.
Statement introduced in Junos OS Release 16.1 for EX Series switches.

Description Configure IPv6 access security options.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Stateless IPv6 Router Advertisement Guard on page 517](#)
- [Configuring Stateful IPv6 Router Advertisement Guard on page 514](#)

action-priority

Syntax	<code>action-priority value;</code>
Hierarchy Level	<code>[edit vlans <i>vlan-name</i> switch-options mac-move-limit interface <i>interface-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 15.1 for EX Series switches.
Description	<p>Configure a priority for an interface on which the MAC move limit action will be applied. When a MAC move limit is configured, and a MAC address moves to a new interface more times than is allowed by the limit, the configured action will be applied to the interface associated with that MAC address having the highest priority. The interface with the highest priority is the interface with the lowest value configured for action-priority. The default value for action-priority on an interface is 4.</p> <p>If no action priority is configured, or if the interfaces have the same action priority, then the action will be applied to the interface to which the MAC address moved last.</p>
Default	The default value for action-priority on an interface is 4.
Required Privilege Level	system—To view this statement in the configuration. system—control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Port Security (non-ELS) on page 15• Configuring MAC Move Limiting (ELS) on page 365• Configuring Autorecovery for Port Security Events on page 635

action-shutdown

Syntax	<code>action-shutdown;</code>
Hierarchy Level	<ul style="list-style-type: none"> For platforms with Enhanced Layer 2 Software (ELS): <code>[edit forwarding-options storm-control-profiles <i>profile-name</i>]</code> For platforms without ELS: <code>[edit ethernet-switching-options storm-control]</code>
Release Information	<p>Statement introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Hierarchy level <code>[edit forwarding-options]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p>
Description	<p>Logically shut down or temporarily disable interfaces when the storm control level is exceeded.</p> <p>To configure the shutdown action so that the interfaces are disabled temporarily, and recover automatically after a specified period of time:</p> <ul style="list-style-type: none"> Configure both the action-shutdown and the port-error-disable statements. The interfaces recover automatically when the disable timeout expires. (The port-error-disable statement is not supported on QFX Series switches or MX Series routers.) Configure both the action-shutdown and the recovery-timeout statements. The interfaces recover automatically when the recovery timeout expires. <p>If you configure the action-shutdown statement and do not configure the port-error-disable or recovery-timeout statement, the interfaces that are enabled for storm control are shut down when the storm control level is exceeded and they do not recover automatically from that port-error condition.</p> <p>If you do not configure the switch for autorecovery from the disabled condition, you can bring up the disabled interfaces by running one of the following commands:</p> <ul style="list-style-type: none"> (MX Series)—Issue the clear bridge recovery-timeout (QFX Series)—Issue the clear ethernet-switching recovery-timeout (EX Series switches that support ELS)—Issue the clear ethernet-switching recovery-timeout (EX Series switches that do not support ELS)—Issue the clear ethernet-switching port-error



NOTE: On EX4300 switches, **action-shutdown** causes an interface to stop learning MAC addresses and it also drops all incoming packets, but does not disable the physical interface.

Default	The action-shutdown option is not enabled by default. The switching device drops packets for the controlled traffic types if the ingress rate of the combined traffic streams exceeds the specified storm control level. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• recovery-timeout on page 959• clear bridge recovery-timeout on page 1076• clear ethernet-switching recovery-timeout on page 1088• Example: Using Storm Control to Prevent Network (MX Routers) on page 641• Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches• Configuring Autorecovery for Port Security Events on page 635


algorithm (Authentication Keychain)

Syntax	<code>algorithm (hmac-sha-1 md5);</code>
Hierarchy Level	<code>[edit security authentication-key-chains key-chain <i>key-chain-name</i> key <i>key</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Configure the authentication algorithm for IS-IS.
Options	hmac-sha-1 —96-bit hash-based message authentication code (SHA-1). md5 —Message digest 5. Default: md5
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i> • <i>Understanding Hitless Authentication Key Rollover for IS-IS</i>

algorithm (Junos FIPS)

Syntax	<code>algorithm 3des-cbc;</code>
Hierarchy Level	<code>[edit security ipsec internal security-association manual direction encryption]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Select the encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPsec security association (SA) configuration.
Options	Only 3des-cbc is supported.
Required Privilege Level	Crypto Officer—To add and view this statement in the configuration.

allowed-mac

Syntax	<pre>allowed-mac { mac-address-list; }</pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify particular MAC addresses to be added to the MAC address cache.
	<div>  <p>NOTE: Although this configuration restricts the addresses that can be added to the MAC address cache, it does not block the switch from receiving Layer 2 control packets—such as Link Layer Discovery Protocol (LLDP) packets—transmitted from MAC addresses that are not specified in the list of allowed MAC addresses. Control packets do not undergo the MAC address check and they are therefore included in the statistics of packets received. However, they are not forwarded to another destination. They are trapped within the switch.</p> </div>
Default	Allowed MAC addresses take precedence over dynamic MAC values that have been applied with the mac-limit statement.
Options	mac-address-list —One or more MAC addresses configured as allowed MAC addresses for a specified interface or all interfaces.
Required Privilege Level	system—To view this statement in the configuration. system—control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • mac-limit (Access Port Security) on page 852 • Example: Configuring Port Security (non-ELS) on page 15 • Example: Protecting Against DHCP Snooping Database Attacks on page 415 • Example: Protecting against Ethernet Switching Table Overflow Attacks on page 354 • Example: Protecting against DHCP Starvation Attacks on page 347 • Configuring MAC Limiting (non-ELS) on page 341 • Configuring MAC Limiting (J-Web Procedure) on page 346

arp-inspection

Syntax

```
arp-inspection {
    forwarding-class class-name;
}
```

Hierarchy Level

- For platforms with ELS:

```
[edit vlans vlan-name forwarding-options dhcp-security],
[edit forwarding-options dhcp-relay ]
```

- For platforms without ELS:

```
[edit ethernet-switching-options secure-access-port vlan (all | vlan-name)],
[edit forwarding-options dhcp-relay ]
```

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security]** introduced in Junos OS Release 13.2X50-D10. (See *Using the Enhanced Layer 2 Software CLI* for information about ELS.)
Statement introduced in Junos OS Release 13.2 for the QFX series.

Description Perform dynamic ARP inspection (DAI) on all VLANs or on the specified VLAN.

When DAI is enabled, the switch logs invalid ARP packets that it receives on each interface, along with the sender's IP and MAC addresses. ARP probe packets, which have the sender IP address 0.0.0.0, are validated by DAI.



NOTE: If you configure DAI at the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level:

- DAI can be configured only for a specific VLAN, not for a list or a range of VLAN IDs.
- DHCP snooping is automatically enabled on the specified VLAN.
- The **forwarding-class** statement is not available at the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level.

See “[Enabling Dynamic ARP Inspection \(ELS\)](#)” on page 451 for more information about this configuration.



NOTE: On EX9200 switches, DAI is not supported in an MC-LAG scenario.

The remaining statement is explained separately.

Default	Disabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks on page 406• Example: Protecting Against ARP Spoofing Attacks on page 418• Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487• Example: Prioritizing Snooped and Inspected Packet on page 423• Enabling Dynamic ARP Inspection (non-ELS) on page 452• Enabling Dynamic ARP Inspection (J-Web Procedure)

arp-inspection (MX Series)

Syntax	arp-inspection;
Hierarchy Level	[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]
Release Information	Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	<p>Perform dynamic ARP inspection (DAI).</p> <p>DAI can only be configured for a specific bridge domain, not for a list or a range of bridge domain names.</p> <p>DHCP snooping is automatically enabled on the specified VLAN or bridge domain.</p>
Default	Disabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Applying CoS Forwarding Classes to Prioritize Inspected Packets on page 453• Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 497

authentication (Security IPsec)

Syntax

```
authentication {
  algorithm (hmac-sha1-96 | hmac-sha2-256);
  key (ascii-text key | hexadecimal key);
}
```

Hierarchy Level [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure IP Security (IPsec) authentication parameters for manual security association (SA).



NOTE: The hexadecimal format must be used for the encryption key to be FIPS compliant. The hexadecimal keys provide maximum key strength.

Options **algorithm**—Hash algorithm that authenticates packet data. It can be one of the following:

- **hmac-md5-96**—Produces a 128-bit digest.
- **hmac-sha1-96**—Produces a 160-bit digest.

key—Type of authentication key. It can be one of the following:

- **ascii-text *key***—ASCII text key. For **hmac-md5-96**, the key is 16 ASCII characters; for **hmac-sha1-96**, the key is 20 ASCII characters.
- **hexadecimal *key***—Hexadecimal key. For **hmac-md5-96**, the key is 32 hexadecimal characters; for **hmac-sha1-96**, the key is 40 hexadecimal characters.

Required Privilege Level **admin**—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Manual IPsec Security Associations for an ES PIC on page 39](#)

authentication-algorithm (Security IKE)

Syntax	authentication-algorithm (md5 sha1);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the Internet Key Exchange (IKE) authentication algorithm.
Options	<p>authentication-algorithm—Hash algorithm that authenticates packet data. It can be one of two algorithms:</p> <ul style="list-style-type: none">• md5—Produces a 128-bit digest.• sha1—Produces a 160-bit digest.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Authentication Algorithm for an IKE Proposal</i>

authentication-algorithm (Security IPsec)

Syntax	<code>authentication-algorithm (hmac-md5-96 hmac-sha1-96);</code>
Hierarchy Level	<code>[edit security ipsec proposal <i>ipsec-proposal-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the IPsec authentication algorithm.



NOTE: Keep the following points in mind when you configure the authentication algorithm in an IPsec proposal:

- When both ends of an IPsec VPN tunnel contain the same IKE proposal but different IPsec proposals, an error occurs and the tunnel is not established in this scenario. For example, if one end of the tunnel contains router 1 configured with the authentication algorithm as hmac-sha-256-128 and the other end of the tunnel contains router 2 configured with the authentication algorithm as hmac-md5-96, the VPN tunnel is not established.
- When both ends of an IPsec VPN tunnel contain the same IKE proposal but different IPsec proposals, and when one end of the tunnel contains two IPsec proposals to check whether a less secure algorithm is selected or not, an error occurs and the tunnel is not established. For example, if you configure two authentication algorithms for an IPsec proposal as hmac-sha-256-128 and hmac-md5-96 on one end of the tunnel, router 1, and if you configure the algorithm for an IPsec proposal as hmac-md5-96 on the other end of the tunnel, router 2, the tunnel is not established and the number of proposals mismatch.
- When you configure two IPsec proposals at both ends of a tunnel, such as the authentication-algorithm hmac-sha-256-128 and authentication-algorithm hmac-md5-96 statements at the `[edit services ipsec-vpn ipsec proposal proposal-name]` hierarchy level on one of the tunnel, router 1 (with the algorithms in two successive statements to specify the order), and the authentication-algorithm hmac-md5-96 and authentication-algorithm hmac-sha-256-128 statements at the `[edit services ipsec-vpn ipsec proposal proposal-name]` hierarchy level on one of the tunnel, router 2 (with the algorithms in two successive statements to specify the order, which is the reverse order of router 1), the tunnel is established in this combination as expected because the number of proposals is the same on both ends and they contain the same set of algorithms. However, the authentication algorithm selected is hmac-md5-96 and not the stronger algorithm of hmac-sha-256-128. This method of selection of the algorithm occurs because the first matching proposal is selected. Also, for a default proposal,

regardless of whether the router supports the Advanced Encryption Standard (AES) encryption algorithm, the 3des-cbc algorithm is chosen and not the aes-cfb algorithm, which is because of the first algorithm in the default proposal being selected. In the sample scenario described here, on router 2, if you reverse the order of the algorithm configuration in the proposal so that it is the same order as the one specified on router 1, hmac-sha-256-128 is selected as the authentication method.

- You must be aware of the order of proposals in an IPsec policy at the time of configuration if you want the matching of proposals to happen in a certain order of preference, such as the strongest algorithm to be considered first when a match is made when both policies from the two peers have a proposal.

Options	authentication-algorithm —Hash algorithm that authenticates packet data. It can be one of two algorithms: <ul style="list-style-type: none">• hmac-md5-96—Produces a 128-bit digest.• hmac-sha1-96—Produces a 160-bit digest.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Authentication Algorithm for an IPsec Proposal on page 47

authentication-key-chains

Syntax	<pre> authentication-key-chains { key-chain key-chain-name { description text-string; key key { algorithm (md5 hmac-sha-1); options (basic isis-enhanced); secret secret-data; start-time yyyy-mm-dd.hh:mm:ss; } tolerance seconds; } } </pre>
Hierarchy Level	[edit security]
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos Limited edition for Junos OS Releases 16.1R7, 16.2R3, 17.1R3, 17.2R3, 17.3R3, and 17.4R2.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in JUNOS OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure authentication key updates for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol. When the authentication-key-chains statement is configured at the [edit security] hierarchy level, and is associated with the BGP, LDP, or IS-IS protocols at the [edit protocols] hierarchy level or with the BFD protocol using the bfd-liveness-detection statement, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <i>Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols</i> <i>Example: Configuring BFD Authentication for Securing Static Routes</i> <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

authentication-method

Syntax	authentication-method (dsa-signatures pre-shared-keys rsa-signatures);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the IKE authentication method.
Options	<p>dsa-signatures—Digital Signature Algorithm (DSA)</p> <p>rsa-signatures—A public key algorithm, which supports encryption and digital signatures</p> <p>pre-shared-keys—A key derived from an out-of-band mechanism; the key authenticates the exchange</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Manual IPsec Security Associations for an ES PIC on page 39• <i>authentication-method (SRX Series)</i>


auto-re-enrollment

Syntax	<pre> auto-re-enrollment { certificate-id { ca-profile <i>ca-profile-name</i>; challenge-password <i>password</i>; re-enroll-trigger-time-percentage <i>percentage</i>; re-generate-keypair; validity-period <i>days</i>; } } </pre>
Hierarchy Level	[edit security pki]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify auto-reenrollment parameters for a certificate authority (CA) issued router certificate. Auto-reenrollment requests that the issuing CA replace a router certificate before its specified expiration date.
Options	The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Auto-Reenrollment of a Router Certificate on page 191 • Configuring Digital Certificates for Adaptive Services Interfaces on page 185

auxiliary-spi (Security IPsec)

Syntax	<code>auxiliary-spi <i>auxiliary-spi-value</i>;</code>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bi-directional)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the auxiliary Security Parameter Index (SPI) for a manual SA. Use the auxiliary SPI when you configure the protocol statement to use the bundle option.
Options	<i>auxiliary-spi-value</i> —Arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet). Range: 256 through 16,639
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Manual IPsec Security Associations for an ES PIC on page 39• spi on page 1002

bandwidth


Syntax	<code>bandwidth <i>bandwidth</i>;</code>
Hierarchy Level	[edit <code>ethernet-switching-options storm-control interface</code> (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.5 for EX Series switches.
Description	<p>Configure the storm control level as the bandwidth in kilobits per second of the applicable traffic streams, as follows:</p> <ul style="list-style-type: none"> On EX2200, EX3200, EX3300, EX4200, and EX6200 switches—Applies to the combined broadcast and unknown unicast streams by default. Storm control does not apply to multicast traffic by default on these switches. If you enable storm control for multicast traffic on a specific interface, the configured bandwidth allocation applies to the combined broadcast, unknown unicast, and multicast traffic on that interface. On EX4500 and EX8200 switches—Applies to the combined broadcast, multicast, and unknown unicast streams.
	<p> NOTE: When you configure storm control bandwidth on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control bandwidth of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.</p>
Default	If you omit the bandwidth statement when you configure storm control on an interface, the storm control level defaults to 80 percent of the available bandwidth used by the combined applicable traffic streams. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic.
Options	<p>bandwidth—Traffic rate in kilobits per second of the combined applicable traffic streams.</p> <p>Range: 100 through 10,000,000</p> <p>Default: None</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [level on page 836](#)
 - [Configuring Autorecovery for Port Security Events on page 635](#)
 - [Enabling and Disabling Storm Control \(non-ELS\) on page 626](#)

bandwidth (DDoS)


Syntax	<code>bandwidth <i>packets-per-second</i>;</code>
Hierarchy Level	<ul style="list-style-type: none"> • For MX Series routers, T4000 routers, and EX9200 switches: <pre>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]</pre> • For PTX Series routers and QFX Series switches: <pre>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]</pre>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.</p> <p>Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.</p>
Description	Configure the DDoS bandwidth rate limit; that is, the maximum traffic rate (packets per second) allowed by the specified policer. When the value is exceeded, a violation is declared.
Options	<p><i>packets-per-second</i>—Number of packets per second that are allowed by the aggregate or packet-type policer.</p> <p>Range: 1 through 100,000 packets per second</p> <p>Default: The default bandwidth value varies by packet type or protocol. You can view the default values for all packet types or protocols before you begin DDoS protection configuration by entering the show ddos-protection protocols parameters brief command from operational mode. For PTX Series routers and QFX Series switches, the default bandwidth limits are also provided in protocols (DDoS) (PTX Series and QFX Series).</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537

bandwidth-level

Syntax	<code>bandwidth-level <i>kbps</i>;</code>
Hierarchy Level	[edit forwarding-options storm-control-profiles <i>profile-name</i> all]
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX Series. Statement introduced in Junos OS Release 14.1 for MX Series routers.
Description	Configure the storm control level as the bandwidth in kilobits per second of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.
	<div>  <p>NOTE: When you configure storm control level on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control level of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.</p> </div>
Default	<p>On EX4300 switches—If you do not specify the storm control level using either the bandwidth-level or the bandwidth-percentage statements, the storm control level defaults to 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.</p> <p>On EX9200 switches—Storm control is not enabled by default.</p> <p>On MX Series routers—Storm control is not enabled by default.</p>
Options	<p>bandwidth-level <i>kbps</i>—Traffic rate in kilobits per second of the combined broadcast, multicast, and unknown unicast traffic streams.</p> <p>Range: 100 through 10,000,000</p> <p>Range: 100 through 100,000,000 on QFX10000 Series switches</p> <p>Default: None</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [bandwidth-percentage on page 685](#)
 - *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
 - [Example: Using Storm Control to Prevent Network \(MX Routers\) on page 641](#)
 - [Enabling and Disabling Storm Control \(ELS\) on page 630](#)

bandwidth-percentage

Syntax	<code>bandwidth-percentage <i>percentage</i>;</code>
Hierarchy Level	[edit forwarding-options storm-control-profiles <i>profile-name</i> all]
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX series. Statement introduced in Junos OS Release 14.1 for MX Series routers.
Description	Configure the storm control level as the percentage of available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams on an interface. The storm control level is configured as part of the storm control profile.
	<div>  <p>NOTE: When you configure storm control level on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control level of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.</p> </div>
Default	<p>On EX4300 switches—The storm control level is 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.</p> <p>On EX9200 switches—Storm control is not enabled by default.</p> <p>On MX Series routers—Storm control is not enabled by default.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • bandwidth-level on page 683 • Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches • Example: Using Storm Control to Prevent Network (MX Routers) on page 641 • Enabling and Disabling Storm Control (ELS) on page 630

bandwidth-scale (DDoS)

Syntax	<code>bandwidth-scale <i>percentage</i>;</code>
Hierarchy Level	<code>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>) fpc <i>slot-number</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.</p> <p>Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.</p>
Description	(MX Series routers with only MPCs, T4000 routers with only FPC5s, PTX Series routers, EX9200 switches, or QFX Series switches) Configure the percentage by which the DDoS bandwidth rate limit is scaled down for the aggregate or packet-type policer on the card in the specified slot.
Options	<p><i>percentage</i>—Percentage multiplied by the bandwidth rate limit to reduce the number of packets per second allowed for the packet type or protocol.</p> <p>Range: 1 through 100 percent</p> <p>Default: 100</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537

bridge-domains

Syntax

```
bridge-domains {
  bridge-domain-name {
    bridge-options {
      ...bridge-options-configuration...
    }
    domain-type bridge;
    interface interface-name;
    no-irb-layer-2-copy;
    no-local-switching;
    routing-interface routing-interface-name;
    vlan-id (all | none | number);
    vlan-id-list [ vlan-id-numbers ];
    vlan-tags outer number inner number;
    bridge-options {
      interface interface-name {
        mac-pinning
        static-mac mac-address;
      }
      interface-mac-limit limit;
      mac-statistics;
      mac-table-size limit;
      no-mac-learning;
    }
  }
}
```

Hierarchy Level [edit],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*],
[edit routing-instances *routing-instance-name*]

Release Information Statement introduced in Junos OS Release 8.4.
Support for logical systems added in Junos OS Release 9.6.
Support for the **no-irb-layer-2-copy** statement added in Junos OS Release 10.2.

Description (MX Series routers only) Configure a domain that includes a set of logical ports that share the same flooding or broadcast characteristics in order to perform Layer 2 bridging.

Options *bridge-domain-name*—Name of the bridge domain.



NOTE: You cannot use the slash (/) character as part of the bridge domain name. If you do, the configuration will not commit.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring a Bridge Domain*
- *Configuring a Layer 2 Virtual Switch*

burst (DDoS)

Syntax `burst size;`

Hierarchy Level • For MX Series routers, T4000 routers, and EX9200 switches:

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
```

• For PTX Series routers and QFX Series switches:

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
```

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.
Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, PTX Series routers, EX9200 switches, or QFX Series switches) Configure the DDoS burst limit; that is, the maximum number of packets that is allowed in a burst of traffic by the specified policer. When this value is exceeded, a violation is declared.

Options **size**—Number of packets that are allowed in a burst by the aggregate or packet-type policer.

Range: 1 through 100,000 packets

Default: The default burst value varies by packet type or protocol. You can view the default values for all packet types or protocols on an unconfigured router or switch by entering the **show ddos-protection protocols parameters brief** command from operational mode. For PTX Series routers and QFX Series switches, the default bandwidth limits are also provided in the [protocols \(DDoS\) \(PTX Series and QFX Series\)](#) statement description.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.


Related Documentation

- [Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537](#)

burst-scale (DDoS)

Syntax	<code>burst-scale <i>percentage</i>;</code>
Hierarchy Level	<code>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>) fpc <i>slot-number</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.</p> <p>Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.</p>
Description	(MX Series routers with only MPCs, T4000 routers with only FPC5s, PTX Series routers, EX9200 switches, or QFX Series switches) Configure the percentage by which the DDoS burst limit is scaled down for the aggregate or packet-type policer on the card in the specified slot.
Options	<p><i>percentage</i>—Percentage multiplied by the burst limit to reduce the number of packets allowed in a burst for the packet type or protocol.</p> <p>Range: 1 through 100 percent</p> <p>Default: 100</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537

bypass-aggregate (DDoS)

Syntax	bypass-aggregate;
Hierarchy Level	<ul style="list-style-type: none"> For MX Series routers, T4000 routers, and EX9200 switches: <pre>[edit system ddos-protection protocols protocol-group packet-type]</pre> For QFX10000 Series and QFX5200 switches: <pre>[edit system ddos-protection protocols protocol-group packet-type]</pre>
	<p> NOTE: The <code>bypass-aggregate</code> option is not supported on PTX Series routers and QFX10002-60C switches.</p>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.</p>
Description	Prevent this packet type from being considered by the DDoS aggregate policer. Traffic for the packet type is still included in traffic statistics.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring DDoS Protection on page 535

cache-size


Syntax	cache-size <i>bytes</i> ;
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the cache size for digital certificates.
Options	bytes —Cache size for digital certificates. Range: 64 through 4,294,967,295 Default: 2 megabytes (MB)



NOTE: We recommend that you limit your cache size to 4 MB.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration
Related Documentation	<ul style="list-style-type: none"> • Configuring the Cache Size on page 180

cache-timeout-negative

Syntax	cache-timeout-negative <i>seconds</i> ;
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure a negative cache for digital certificates.
Options	seconds —Negative time to cache digital certificates, in seconds. Range: 10 through 4,294,967,295 Default: 20
<div> CAUTION: Configuring a large negative cache value can lead to a denial-of-service attack.</div>	
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration
Related Documentation	<ul style="list-style-type: none">• Configuring the Negative Cache on page 180

ca-identity

Syntax	<code>ca-identity <i>ca-identity</i>;</code>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	Specify the certificate authority (CA) identity to use in requesting digital certificates for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M Series and T Series routers.
Options	<i>ca-identity</i> —The name of the CA identity. This name is typically the domain name of the CA.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the CA Profile Name on page 187

cak

Syntax	<code>ckn <i>hexadecimal-number</i>;</code>
Hierarchy Level	<pre>[edit security macsec connectivity-association connectivity-association-name pre-shared-key], [edit security macsec connectivity-association connectivity-association-name fallback-key]</pre>
Release Information	<p>Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.</p> <p>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.</p>
Description	<p>Specifies the connectivity association key (CAK) for a preshared key.</p> <p>A preshared key includes a connectivity association key name (CKN) and a CAK. A preshared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using dynamic security keys. The MACsec Key Agreement (MKA) protocol is enabled once the preshared keys are successfully exchanged. The preshared key—the CKN and CAK—must match on both ends of a link.</p>
Default	No CAK exists, by default.
Options	<p><i>hexadecimal-number</i>—The key name, in hexadecimal format.</p> <p>The key name is 32 hexadecimal characters in length. To maximize security, we recommend configuring all 32 digits of a CAK. If you enter a key name that is less than 32 characters long, the remaining characters are set to 0. However, you will receive a warning message when you commit the configuration.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

cak (MX Series)

Syntax	<code>cak <i>hexadecimal-number</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> pre-shared-key]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers. Statement introduced in Junos OS Release 17.3R1 for MX10003 Universal Routing Platforms.
Description	<p>Specifies the connectivity association key (CAK) for a pre-shared key.</p> <p>A pre-shared key includes a connectivity association key name (CKN) and a CAK. A pre-shared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using dynamic security keys. The MACsec Key Agreement (MKA) protocol is enabled once the pre-shared keys are successfully exchanged. The pre-shared key—the CKN and CAK—must match on both ends of a link</p>
Default	No CAK exists, by default.
Options	<p><i>hexadecimal-number</i>—The key name, in hexadecimal format.</p> <p>The key name is 32 hexadecimal characters in length. If you enter a key name that is less than 32 characters long, the remaining characters are set to 0.</p> <p>On MX10003 router, to maximize the security, it is recommended to configure CAK of even length.</p> <ul style="list-style-type: none"> If you configure CAK of length that is less than 32 hexadecimal digits and if cipher-suite is gcm-aes-128/gcm-aes-256 and less than 64 hexadecimal digits, then the following warning message is displayed: warning: To maximize security, recommend configuring all 32 digits of pre-shared-key cak or warning: To maximize security, recommend configuring all 64 digits of pre-shared-key cak On MX10003 router, if you configure the length of CAK to an odd value, then the following warning message is displayed: To maximize security, it is recommended to configure pre-shared-key cak of even length
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

ca-name

Syntax	<code>ca-name <i>ca-identity</i>;</code>
Hierarchy Level	[edit security certificates certification-authority]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the certificate authority (CA) identity to use in the certificate request.
Options	<i>ca-identity</i> —CA identity to use in the certificate request.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Certificate Authority Name on page 178

ca-profile (Security PKI)

```
Syntax  ca-profile ca-profile-name {
        administrator {
            e-mail-address e-mail-address;
        }
        ca-identity ca-identity;
        enrollment {
            retry number;
            retry-interval seconds;
            url url-name;
        }
        revocation-check {
            disable;
            crl {
                disable {
                    on-download-failure;
                }
                refresh-interval hours;
                url url-name;
            }
            disable;
            ocsf {
                connection-failure (disable | fallback-crl);
                disable-responder-revocation-check;
                nonce-payload (enable | disable);
                url ocsp-url;
            }
            use-ocsp;
        }
        routing-instance routing-instance-name;
        source-address ip-address;
    }
```

Hierarchy Level [edit security pki]

Release Information Statement modified in Junos OS Release 8.5. Support for **ocsp** and **use-ocsp** options added in Junos OS Release 12.1X46-D20.

Description Configure certificate authority (CA) profile.

Options *ca-profile-name* —Name of a trusted CA.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

- Related Documentation**
- [Understanding Certificates and PKI](#)

certificate-id

Syntax

```
certificate-id {  
  ca-profile ca-profile-name;  
  challenge-password password;  
  re-enroll-trigger-time-percentage percentage;  
  re-generate-keypair;  
  validity-period days;  
}
```

Hierarchy Level [edit security [auto-re-enrollment](#)]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify a router certificate for auto-reenrollment. The ID is the same as that used to get the end entity's certificate from the issuing certificate authority.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

admin	—To view this statement in the configuration.
admin-control	—To add this statement to the configuration.

- Related Documentation**
- [Configuring Auto-Reenrollment of a Router Certificate on page 191](#)
 - [auto-re-enrollment on page 679](#)

certificates

Syntax

```

certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl file-name;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
  }
  maximum-certificates number;
  path-length certificate-path-length;
}

```

Hierarchy Level [edit security]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only)
Configure the digital certificates for IPsec.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Digital Certificates for an ES PIC on page 177](#)

certification-authority

Syntax	<pre> certification-authority <i>ca-profile-name</i> { <i>ca-name</i> <i>ca-identity</i>; <i>crl</i> <i>file-name</i>; <i>encoding</i> (binary pem); <i>enrollment-url</i> <i>url-name</i>; <i>file</i> <i>certificate-filename</i>; <i>ldap-url</i> <i>url-name</i>; } </pre>
Hierarchy Level	[edit security certificates]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced before Junos OS Release 12.1 for the SRX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>(Encryption interface on M Series and T Series routers and EX Series switches only)</p> <p>Configure a certificate authority profile name.</p> <p>Configure certification authority (CA) for X.509 certificate.</p>
Options	<ul style="list-style-type: none"> <i>profile-name</i>—Name of this CA configuration. <i>ca-name</i> <i>name</i>—Name of the CA. <i>crl</i> <i>filename</i>—Certificate revocation list (CRL) filename. <i>encoding</i>—Certificate encoding, either binary or pem (privacy-enhanced mail). <i>enrollment-url</i> <i>url</i>—Enrollment URL. <i>file</i> <i>filename</i>—Certificate filename. <i>ldap-url</i> <i>url</i>—Lightweight Directory Access Protocol (LDAP) URL.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration</p>
Related Documentation	<ul style="list-style-type: none"> Configuring the Certificate Authority Properties for an ES PIC on page 178 Configuring the Certificate Authority Properties for an ES PIC on page 178

challenge-password

Syntax	<code>challenge-password <i>password</i>;</code>
Hierarchy Level	[edit security pki auto-re-enrollment certificate-id]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the challenge password used by the certificate authority (CA) for router certificate enrollment and revocation. This challenge password must be the same used when the router certificate was originally configured.
Options	<i>password</i> —The password required by the CA.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Auto-Reenrollment of a Router Certificate on page 191• auto-re-enrollment on page 679

children

```
Syntax children {
    child-name {
        esp-proposal esp-proposal;
        local-traffic-selector {
            (ipv4-prefix ipv4-prefix | ipv6-prefix ipv6-prefix);
            port port;
            protocol protocol;
        }
        mode (transport | tunnel);
        rekey-time rekey-time;
        remote-traffic-selector {
            (ipv4-prefix ipv4-prefix | ipv6-prefix ipv6-prefix);
            port port;
            protocol protocol;
        }
    }
}
```

Hierarchy Level [edit security host-vpn connections *connection-name*]

Release Information Statement introduced in Junos OS Evolved Release 18.3R1.

Description Configure child details to establish a security association (SA). An SA describes a specific negotiated set of parameters to protect traffic between two host for a certain period of time.

Options *child-name*—Specify the child SA name.

esp-proposal *esp-proposal*—Specify the algorithms to use in negotiating the child SA from among the pre-selected combinations available, which represent the encryption algorithm, integrity algorithm, and Diffie Hellman group. There are the following options:

3des-sha1-modp1536—Propose 3des SHA1 and DH group modp1536.

aes256gcm128-ecp384—Propose aes256gcm128 and DH group ecp384.

aes256gcm128-modp3072—Propose aes256gcm128 and DH group modp3072.

aes256-sha384-ecp384—Propose aes256 CBC, sha384 and DH group ecp384.

aes256-sha384-modp3072—Propose aes256 CBC, sha384 and DH group modp3072.

[]—Propose a set composed from the values permitted.

Default: aes256gcm128-ecp384

mode (transport | tunnel)—Specify the IPsec usage mode to negotiate: **transport** or **tunnel**.

tunnel—In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode may be used with any kind of IP traffic. Of the two modes, only tunnel mode supports NAT transversal. Tunnel mode is required if you are communicating with a server behind a gateway.

transport—In transport mode, only the payload of the IP packet is encrypted or authenticated. The IP header is neither modified nor encrypted. Transport mode does not support NAT transversal. Transport mode or tunnel mode can be used when communications is between two hosts, for example, between a router and a Syslog server.

Default: tunnel

rekey-time *rekey-time*—Specify how long, in seconds, before the child SA is rekeyed. Actual rekeying occurs slightly sooner than the rekey time specified because of rekey randomization.



Default: 14,400

Range: 60 through 86,400

The remaining statements are explained separately.

Required Privilege	security—To view this statement in the configuration.
Level	security-control—To add this statement to the configuration.

cipher-suite (MACsec)

Syntax	<code>cipher-suite <i>encryption-algorithm-name</i>;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 16.2R1 for MX240, MX480, MX960, MX2020, and MX2010 routers.</p> <p>Statement introduced in Junos OS Release 17.2R1 for QFX Series switches.</p> <p>Statement introduced in Junos OS Release 17.3R1 for JNP-MIC1-MACSEC MIC on MX10003 routers.</p> <p>Statement introduced in Junos OS Release 18.2R1 for EX Series switches.</p>
Description	<p>Specify the set of ciphers used to encrypt traffic on an Ethernet link that is secured with Media Access Control Security (MACsec). The encryption used by MACsec ensures that the data in the Ethernet frame cannot be viewed by anybody monitoring traffic on the link. MACsec encryption is optional and user-configurable. The configured cipher suites should be the same between MACsec peers.</p> <p>MACsec utilizes the Galois/Counter Mode Advanced Encryption Standard (GCM-AES). The default cipher suite used for MACsec is GCM-AES-128, with a maximum key length of 128 bits. MACsec also supports GCM-AES-256, with a maximum key length of 256 bits.</p> <p>GCM-AES-128 and GCM-AES-256 use a 32-bit packet number as part of the initial value that has to be unique for every packet sent with a given secure association key (SAK). When the permutations of the 32-bit packet number are exhausted, the SAK must be refreshed. The frequency of SAK refreshes can be reduced by using a cipher suite with Extended Packet Numbering (XPN), which increases the size of the packet number to 64-bits. Both GCM-AES-128 and GCM-AES-256 are available with XPN.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;"> <p> NOTE: When enabling MACsec on <i>et</i> interfaces, use either the GCM-AES-XPN-128 or GCM-AES-XPN-256 cipher suite.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;"> <p> NOTE: On EX4300-48MP switches, the XPN cipher suites are not supported on multi-rate ports.</p> </div>
Default	If the cipher-suite statement is not configured, the default cipher suite used for encryption is GCM-AES-128.
Options	gcm-aes-128 —GCM-AES-128 has a maximum key size of 128 bits.

gcm-aes-xpn-128—GCM-AES-XPB-128 has a maximum key size of 128 bits and extended packet number.

gcm-aes-256—GCM-AES-256 has a maximum key size of 256 bits.

gcm-aes-xpn-256—GCM-AES-XPB-256 has a maximum key size of 256 bits and extended packet number.

Required Privilege Level	admin— To view this statement in the configuration. admin-control— To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228• Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268
------------------------------	--

circuit-id

Syntax

```
circuit-id {
  prefix {
    host-name;
    logical-system-name;
    routing-instance-name;
  }
  use-interface-description (device | logical);
  use-vlan-id;
}
```

- Hierarchy Level**
- For platforms with Enhanced Layer 2 Software (ELS):

```
[edit vlans vlan-name forwarding-options dhcp-security option-82 ]
```

- For MX Series platforms:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security option-82]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
 Statement introduced in Junos OS Release 11.3 for the QFX Series.
 Hierarchy level `[edit vlans vlan-name forwarding-options dhcp-security]` introduced in Junos OS Release 13.2X50-D10. (See *Using the Enhanced Layer 2 Software CLI* for information about ELS.)
 Statement introduced in Junos OS Release 14.1 for the MX Series.
 Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the **circuit-id** suboption (suboption 1) of DHCP option 82 (the DHCP relay agent information option) in DHCP packets destined for a DHCP server. This suboption identifies the circuit (the interface, the VLAN, or both) on which the DHCP request arrived.

The remaining statements are explained separately. See [CLI Explorer](#).

Default

If DHCP option 82 is enabled on the switch, the circuit ID is supplied by default in the format *interface-name:vlan-name* or, on a Layer 3 interface, just *interface-name*.



NOTE: When you configure **circuit-id**, **remote-id** is also enabled, even if you do not explicitly configure **remote-id**.

Required Privilege Level

system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

- Related Documentation**
- [Example: Setting Up DHCP Option 82 on page 433](#)
 - RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>

ckn

Syntax	<code>ckn <i>hexadecimal-number</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name pre-shared-key</i>], [edit security macsec connectivity-association <i>connectivity-association-name fallback-key</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
Description	Specifies the connectivity association key name (CKN) for a preshared key. A preshared key includes a CKN and a connectivity association key (CAK). A preshared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using dynamic security keys. The MACsec Key Agreement (MKA) protocol is enabled once the preshared keys are successfully exchanged. The preshared key—the CKN and CAK—must match on both ends of a link
Default	No CKN exists, by default.
Options	<i>hexadecimal-number</i> —The key name, in hexadecimal format. The key name is 64 hexadecimal characters in length. To maximize security, we recommend configuring all 64 digits of a CKN. If you enter a key name that is less than 64 characters long, the remaining characters are set to 0. However, you will receive a warning message when you commit the configuration.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	• Configuring MACsec on EX, SRX and Fusion Devices on page 228

connections (Host VPN)

```

Syntax connections {
    connection-name {
        children {
            child-name {
                esp-proposal esp-proposal;
                local-traffic-selector {
                    (ipv4-prefix ipv4-prefix | ipv6-prefix ipv6-prefix);
                    port port;
                    protocol protocol;
                }
                mode (transport | tunnel);
                rekey-time rekey-time;
                remote-traffic-selector {
                    (ipv4-prefix ipv4-prefix | ipv6-prefix ipv6-prefix);
                    port port;
                    protocol protocol;
                }
            }
        }
        dpd-delay dpd-delay;
        ike-proposal ike-proposal;
        local {
            id local-id;
        }
        local-address {
            (ipv4 ipv4-address | ipv6 ipv6-address);
        }
        rekey-time rekey-time;
        remote {
            id remote-id;
        }
        remote {
            id remote-id;
        }
        remote-address {
            (ipv4 ipv4-address | ipv6 ipv6-address);
        }
    }
}

```

Hierarchy Level [edit security host-vpn]

Release Information Statement introduced in Junos OS Evolved Release 18.3R1.

Description Configure IPsec connection details. The Internet Key Exchange (IKE) protocol is a component of IPsec used for performing mutual authentication and establishing and maintaining security associations (SAs). Each SA describes a specific negotiated set of parameters to protect traffic for a certain time period for an IPsec VPN.

Options *connection-name*—Specify the name of the IKE SA connection.

dpd-delay—Specify the Dead Peer Detection delay used on the connection. This is the interval between sending liveness messages.

Default: 0, which is disabled Dead Peer Detection.

Range: 0 through 3600

ike-proposal *ike-proposal*—Specify the algorithms to use in negotiating the IKE SA from among the pre-selected combinations available, which represent the encryption algorithm, integrity algorithm, and Diffie Hellman group.

3des-sha1-modp1536—Propose 3des SHA1 and DH group modp1536.

aes256gcm128-ecp384—Propose aes256gcm128 and DH group ecp384.

aes256gcm128-modp3072—Propose aes256gcm128 and DH group modp3072.

aes256-sha384-ecp384—Propose aes256 CBC, sha384 and DH group ecp384.

aes256-sha384-modp3072—Propose aes256 CBC, sha384 and DH group modp3072.

[]—Propose a set composed from the values permitted.

Default: aes256-sha384-ecp384

local-address—Specify the local endpoint's IPv4 or IPv6 address.

rekey-time *rekey-time*—Specify how long in seconds before the IKE SA is rekeyed. Actual rekeying occurs slightly sooner than that specified because of rekey randomization.

Default: 14,400

Range: 60 through 86,400

remote-address—Specify the remote endpoint's IPv4 or IPv6 address.

The remaining statements are explained separately.

Required Privilege	security—To view this statement in the configuration.
Level	security-control—To add this statement to the configuration.

connectivity-association

Syntax

```
connectivity-association connectivity-association-name {
  exclude-protocol protocol-name;
  fallback-key {
    cak hexadecimal-number;
    ckn hexadecimal-number;
  }
  include-sci;
  mka {
    must-secure;
    key-server-priority priority-number;
    transmit-interval interval;
  }
  no-encryption;
  offset (0|30|50);
  pre-shared-key {
    cak hexadecimal-number;
    ckn hexadecimal-number;
  }
  replay-protect{
    replay-window-size number-of-packets;
  }
  secure-channel secure-channel-name {
    direction (inbound | outbound);
    encryption (MACsec);
    id {
      mac-address mac-address;
      port-id port-id-number;
    }
    offset (0|30|50);
    security-association security-association-number {
      key key-string;
    }
  }
  security-mode security-mode;
}
```

Hierarchy Level [edit security **macsec**]

Release Information Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.

Description Create or configure a MACsec connectivity association.

A connectivity association is not applying MACsec to traffic until it is associated with an interface. MACsec connectivity associations are associated with interfaces using the **interfaces** statement in the [edit security macsec] hierarchy.

Default	No connectivity associations are present, by default.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

connectivity-association (MACsec Interfaces)

Syntax	<code>connectivity-association <i>connectivity-association-name</i>;</code>
Hierarchy Level	[edit security <code>macsec interfaces</code> <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	Applies a connectivity association to an interface, which enables Media Access Control Security (MACsec) on that interface.
Default	No connectivity associations are associated with any interfaces.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

connectivity-association (MACsec Interfaces for MX Series)

Syntax	<code>connectivity-association <i>connectivity-association-name</i>;</code>
Hierarchy Level	<code>[edit security macsec interfaces <i>interface-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	Applies a connectivity association to an interface, which enables Media Access Control Security (MACsec) on that interface.
Default	No connectivity associations are associated with any interfaces.
Options	<i>connectivity-association-name</i> —Name of the MACsec connectivity association. Range: 1 through 32 alphanumeric characters. Allowed characters are [a-z, A-Z, 0-9]
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

crl (Adaptive Services Interface)

Syntax	<pre> crl { disable on-download-failure; refresh-interval <i>number-of-hours</i>; url { <i>url-name</i>; password; } } </pre>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i> revocation-check]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.
Options	<p>disable on-download-failure—Permit the authentication of the IPsec peer when the CRL is not downloaded.</p> <p>password—Password to access the URLs.</p> <p>refresh-interval <i>number-of-hours</i>—Time interval, in hours, between CRL updates. Range: 0 through 8784 Default: 24</p> <p>url <i>url-name</i>—Location from which to retrieve the CRL through the Lightweight Directory Access Protocol (LDAP). You can configure as many as three URLs for each configured CA profile.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration</p>
Related Documentation	<ul style="list-style-type: none"> Configuring the Certificate Revocation List on page 188

crl (Encryption Interface)

Syntax	<code>crl <i>file-name</i>;</code>
Hierarchy Level	[edit security certificates]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>(Encryption interface on M Series and T Series routers and EX Series switches only)</p> <p>Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.</p>
Options	<p><i>file-name</i>—Specify the file from which to read the CRL.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Certificate Authority Properties for an ES PIC on page 178

ddos-protection (DDoS)

List of Syntax Syntax (PTX Series Routers and QFX Series Switches) on page 715
 Syntax (Other Routers and EX9200 Switches) on page 715

Syntax (PTX Series Routers and QFX Series Switches)

```
ddos-protection
  global {
    disable-fpc;
    disable-logging;
  }
  protocols protocol-group (aggregate | packet-type) {
    bandwidth packets-per-second;
    burst size;
    bypass-aggregate;
    disable-fpc;
    disable-logging;
    fpc slot-number {
      bandwidth-scale percentage;
      burst-scale percentage;
      disable-fpc;
    }
    priority level;
  }
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
```

Syntax (Other Routers and EX9200 Switches)

```
ddos-protection
  global {
    disable-fpc;
    disable-logging;
    disable-routing-engine;
    flow-detection;
    flow-level-control;
    flow-detection-mode;
    flow-report-rate;
    violation-report-rate;
  }
  protocols protocol-group (aggregate | packet-type) {
    bandwidth packets-per-second;
    burst size;
    bypass-aggregate;
    disable-fpc;
    disable-logging;
    disable-routing-engine;
    flow-detection-mode (automatic | off | on);
    flow-detect-time seconds;
```

```

flow-level-bandwidth {
    logical-interface flow-bandwidth;
    physical-interface flow-bandwidth;
    subscriber flow-bandwidth;
}
flow-level-control {
    logical-interface flow-control-mode;
    physical-interface flow-control-mode;
    subscriber flow-control-mode;
}
flow-level-detection {
    logical-interface flow-detection-mode;
    physical-interface flow-detection-mode;
    subscriber flow-detection-mode;
}
flow-recover-time seconds;
flow-timeout-time seconds;
fpc slot-number {
    bandwidth-scale percentage;
    burst-scale percentage;
    disable-fpc;
}
no-flow-logging
priority level;
recover-time seconds;
timeout-active-flows;
}
traceoptions{
    file filename <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
}

```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.
Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.
Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.

Description Configure DDoS protection policers.

DDoS attacks typically use network control packets to trigger large numbers of exceptions to a device's control plane that disrupts normal network operations. DDoS protection polices traffic to enable the device to continue functioning under a DDoS attack.

DDoS protection is enabled by default on supporting devices for the protocol groups and packet types available on the device. You can disable particular policers or change default policer parameters, including:

- Set the maximum allowed traffic rate, maximum burst size, and traffic priority.
- Define how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack.
- Scale bandwidth and burst values for individual line cards so that the policers at this level trigger at lower thresholds than the overall protocol or packet thresholds.

DDoS protection supports policers for many protocol groups and specific packet types within some protocol groups. Protocol group and packet type support varies across platforms and Junos OS releases. See the **protocols** statement for details on the main differences as follows:

- For PTX Series routers and QFX Series switches, see [protocols \(DDoS\) \(PTX Series and QFX Series\)](#).
- For all other routing devices and EX9200 switches, see [protocols \(DDoS\)](#).

The remaining statements in this configuration statement hierarchy are explained separately. Search for a statement in [CLI Explorer](#) or click a linked statement in the Syntax section for details.



NOTE: PTX Series routers and QFX10002-60C switches do not support the **bypass-aggregate** option.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring DDoS Protection on page 535](#)
- [Configuring Flow Detection for DDoS Protection](#)

description (Authentication Keychain)

Syntax	<code>description <i>text-string</i>;</code>
Hierarchy Level	<code>[edit security authentication-key-chains key-chain <i>key-chain-name</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in JUNOS OS Release 11.2.</p>
Description	Configure a description for an authentication key-chain.
Options	<i>text-string</i> —A text string describing the authentication-key-chain . Put the text string in quotes ("text description").
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols</i>• <i>Example: Configuring BFD Authentication for Securing Static Routes</i>• <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

description (IKE policy)

Syntax	<code>description <i>description</i>;</code>
Hierarchy Level	<code>[edit security ike policy <i>ike-peer-address</i>],</code> <code>[edit security ike proposal <i>ike-proposal-name</i>],</code> <code>[edit security ipsec policy <i>ipsec-policy-name</i>],</code> <code>[edit security ipsec proposal <i>ipsec-proposal-name</i>],</code> <code>[edit security ipsec security-association <i>sa-name</i>]</code>
Description	Specify a text description for an IKE proposal or policy, or an IPsec proposal, policy, or SA.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Security Associations for IPsec on an ES PIC on page 37 • Configuring the Description for an IKE Proposal • Configuring an IKE Policy for Preshared Keys on page 44 • Configuring an IPsec Proposal for an ES PIC on page 47 • Configuring the IPsec Policy for an ES PIC on page 49

dhcp-option82

Syntax	<pre> dhcp-option82 { circuit-id { prefix hostname; use-interface-description; use-vlan-id; } remote-id { prefix hostname mac none; use-interface-description; use-string string; } vendor-id <string>; } </pre>
Hierarchy Level	<pre> [edit ethernet-switching-options secure-access-port vlan (all vlan-name)] [edit forwarding-options helpers bootp] [edit forwarding-options helpers bootp interface interface-name] </pre>
Release Information	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	<p>When the switch receives a DHCP request from a DHCP client connected on one of the switch's interfaces, have the switch insert DHCP option 82 (also known as the DHCP relay agent information option) information in the DHCP request packet header before it forwards or relays the request to a DHCP server. The server uses the option 82 information, which provides details about the circuit and host the request came from, in formulating the reply; the server does not, however, make any changes to the option 82 information in the packet header. The switch receives the reply and then removes the DHCP option 82 information before forwarding the reply to the client.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Default	Insertion of DHCP option 82 information is not enabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443 • Example: Setting Up DHCP Option 82 on page 433 • RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046.

dhcp-security

```
Syntax  dhcp-security {
    arp-inspection;
    dhcpv6-options {
        light-weight-dhcpv6-relay;
        option-16 {
            use-string string;
        }
        option-18 {
            prefix {
                host-name;
                logical-system-name;
                routing-instance-name;
                vlan-id;
                vlan-name;
            }
            use-interface-mac;
            use-interface-index (device | logical);
            use-interface-description (device | logical);
            use-interface-name (device | logical);
            use-string string;
        }
        option-37 {
            prefix {
                host-name;
                logical-system-name;
                routing-instance-name;
                vlan-id;
                vlan-name;
            }
            use-interface-mac;
            use-interface-index (device | logical);
            use-interface-description (device | logical);
            use-interface-name (device | logical);
            use-string string;
        }
    }
    group group-name {
        interface interface-name {
            static-ip ip-address {
                mac mac-address;
            }
            static-ipv6 ip-address {
                mac mac-address;
            }
        }
    }
    overrides {
        no-dhcpv6-options;
        no-option16;
        no-option18;
        no-option37;
        no-option82;
    }
}
```

```

    trusted;
    untrusted;
  }
}
ip-source-guard;
ipv6-source-guard;
neighbor-discovery-inspection;
no-dhcp-snooping;
no-dhcpv6-snooping;
option-82 {
  circuit-id {
    prefix {
      host-name;
      logical-system-name;
      routing-instance-name;
    }
    use-interface-description (device | logical);
    use-vlan-id;
  }
  remote-id {
    host-name hostname;
    use-interface-description (device | logical);
    mac;
    use-string string;
  }
  vendor-id {
    use-string string;
  }
}
}

```

Hierarchy Level [edit vlans *vlan-name* forwarding-options]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX series. Support for **static-ipv6**, **neighbor-discovery-inspection**, **ipv6-source-guard**, **no-dhcpv6-snooping**, and **no-option37** introduced in Junos OS Release 13.2X51-D20 for EX Series switches. Support for **dhcpv6-options**, **option-16**, **option-18**, **option-37**, **no-dhcpv6-options**, **no-option16**, **no-option18**, and **no-option37** introduced in Junos OS Release 14.2 for EX Series switches.

Description Configure DHCP or DHCPv6 snooping on the switch. DHCP snooping is also enabled automatically if you configure any of the following port security features within this hierarchy:

- Dynamic ARP inspection (DAI)
- IP source guard
- DHCP option 82
- Static IP

For switches that support DHCPv6, both DHCP snooping and DHCPv6 snooping are enabled automatically if you configure any of the afore-mentioned features or any of the following IPv6 features:

- IPv6 neighbor discovery inspection
- IPv6 source guard
- Static IPv6



NOTE: On EX9200 switches, DHCP Snooping, DHCPv6 Snooping and Port Security features are not supported in MC-LAG scenario.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Enabling Dynamic ARP Inspection \(ELS\) on page 451](#)
- [Configuring IP Source Guard \(ELS\) on page 465](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\) on page 439](#)
- [Configuring Static DHCP IP Addresses for DHCP snooping \(ELS\) on page 404](#)

dhcp-security (MX Series)

```
Syntax  dhcp-security {
        arp-inspection;
        group group-name {
            interface interface-name {
                static-ip ip-address {
                    mac mac-address;
                }
            }
        }
        overrides {
            no-option82;
            trusted;
            untrusted;
        }
    }
    ip-source-guard;
    no-dhcp-snooping;
    option-82 {
        circuit-id {
            prefix {
                host-name;
                logical-system-name;
                routing-instance-name;
            }
            use-interface-description (device | logical);
            use-vlan-id;
        }
        remote-id {
            host-name;
            use-interface-description (device | logical);
            use-string string;
        }
        vendor-id {
            use-string string;
        }
    }
}
```

Hierarchy Level [edit [bridge-domains](#) *bridge-domain-name* [forwarding-options](#) dhcp-security]

Release Information Statement introduced in Junos OS Release 14.1 for the MX Series.

Description Configure port security features on the switching device. DHCP snooping is enabled automatically if you configure any of the following port security features within this hierarchy:

- Dynamic ARP inspection (DAI)
- IP source guard
- DHCP option 82

- The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level	
system	To view this statement in the configuration.
system-control	To add this statement to the configuration.

Copyright © 2019, Juniper Networks, Inc.

dhcp-service

```

Syntax  dhcp-service {
        accept-max-tcp-connections max-tcp-connections;
        dhcp-snooping-file(local_pathname | remote_URL) {
            write-interval interval;
        }
        dhcpv6-snooping-file {
            location;
            write-interval seconds;
        }
        (disable | enable);
        interface-traceoptions {
            file filename <files number> <match regular-expression > <size maximum-file-size>
            <world-readable | no-world-readable>;
            flag flag;
            level (all | error | info | notice | verbose | warning);
            no-remote-trace;
        }
        log {
            session {
                client;
                all;
                dhcpv6 {
                    client;
                    server;
                    relay;
                    dynamic-server;
                    all;
                }
                server;
                relay;
            }
        }
        ltv-syslog-interval seconds;
        persistent-storage {
            backup-interval backup-interval;
            file-name;
        }
        request-max-tcp-connections max-tcp-connections;
        traceoptions {
            file filename <files number> <match regular-expression > <size maximum-file-size>
            <world-readable | no-world-readable>;
            flag flag;
            level (all | error | info | notice | verbose | warning);
            no-remote-trace;
        }
    }

```

Hierarchy Level [edit system processes]

Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX Series. Statement introduced in Junos OS Release 14.1 for MX Series routers. Support for log option introduced in Junos OS Release 19.1R1 for SRX Series devices.
Description	<p>Enable DHCP services on the device. DHCP services automate network-parameter assignment to network devices. The DHCP service process is enabled by default. However, by default, IP-MAC bindings in the DHCP snooping database do not persist through device reboots. You can improve performance after rebooting by configuring the IP-MAC bindings to persist, by configuring a storage location for the DHCP database file. When specifying the location for the DHCP database, you must also specify how frequently the switch writes the database entries into the DHCP snooping database file.</p> <p>The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Persistent Bindings in the DHCP or DHCPv6 (ELS) on page 381

dhcp-snooping-file

Syntax	<pre>dhcp-snooping-file { location (local_pathname remote_URL); timeout seconds; write-interval seconds; }</pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port]
Release Information	Statement introduced in Junos OS Release 9.4 for EX Series switches.
Description	<p>Ensure that IP-MAC bindings persist through switch reboots by specifying a local pathname or a remote URL for the storage location of the DHCP snooping database file.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Default	The IP-MAC bindings in the DHCP snooping database file are not persistent. If the switch is rebooted, the bindings are lost.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Persistent Bindings in the DHCP or DHCPv6 (non-ELS) on page 383• Understanding DHCP Snooping (non-ELS) on page 393

dhcp-snooping-file

Syntax	<code>dhcp-snooping-file (<i>local_pathname</i> <i>remote_URL</i>); <i>write-interval</i> <i>seconds</i>; }</code>
Hierarchy Level	[edit system processes dhcp-service]
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 14.1 for MX Series routers.
Description	<p>Ensure that IP-MAC bindings persist through the device reboots by specifying a local pathname or a remote URL for the storage location of the DHCP snooping database file. You <i>must</i> specify how frequently the device writes the database entries into the DHCP snooping database file.</p> <p>The remaining statement is explained separately. See CLI Explorer.</p>
Default	The IP-MAC bindings in the DHCP snooping database file are not persistent by default. If the device is rebooted, the bindings are lost, and the table must be rebuilt on reboot.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Persistent Bindings in the DHCP or DHCPv6 (ELS) on page 381 • Configuring Static DHCP IP Addresses for DHCP snooping (MX routers) on page 406 • Understanding DHCP Snooping (non-ELS) on page 393

dhcp-trusted

Syntax	(dhcp-trusted no-dhcp-trusted);
Hierarchy Level	[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Allow DHCP responses from the specified interfaces (ports) or all interfaces.</p> <ul style="list-style-type: none">• dhcp-trusted—Allow DHCP responses.• no-dhcp-trusted—Deny DHCP responses.
Default	Trusted for trunk ports, untrusted for access ports.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Port Security (non-ELS) on page 15• Example: Protecting against Rogue DHCP Server Attacks on page 351• Enabling a Trusted DHCP Server (non-ELS) on page 373

dhcpv6-options

```
Syntax  dhcpv6-options {
        option-16 {
            use-string string;
        }
        option-18 {
            prefix {
                host-name;
                logical-system-name;
                routing-instance-name;
                vlan-id;
                vlan-name;
            }
            use-interface-mac;
            use-interface-index (device | logical);
            use-interface-description (device | logical);
            use-interface-name (device | logical);
            use-string string;
        }
        option-37 {
            prefix {
                host-name;
                logical-system-name;
                routing-instance-name;
                vlan-id;
                vlan-name;
            }
            use-interface-mac;
            use-interface-index (device | logical);
            use-interface-description (device | logical);
            use-interface-name (device | logical);
            use-string string;
        }
    }
```

Hierarchy Level [edit vlans *vlan-name* forwarding-options [dhcp-security](#)]

Release Information Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Configure optional information to be included in DHCPv6 packets during the DHCPv6 snooping process.

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**
- [no-dhcpv6-options on page 879](#)
 - [Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\) on page 439](#)
 - [Configuring Static DHCP IP Addresses for DHCP snooping \(ELS\) on page 404](#)

dhcpv6-snooping-file

Syntax

```
dhcpv6-snooping-file (local_pathname | remote_URL);  
  location local_pathname | remote_URL;  
  timeout seconds;  
  write-interval seconds;  
}
```

- Hierarchy Level**
- For platforms with Enhanced Layer 2 Software (ELS):

```
[edit system processes dhcp-service];
```

- For platforms without ELS:

```
[edit ethernet-switching-options secure-access-port]
```

Release Information Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches. Support at the **[edit ethernet-switching-options secure-access-port]** hierarchy level introduced in Junos OS 14.1X53-D10 for EX Series switches.

Description Ensure that IP-MAC bindings persist through switch reboots by specifying a local pathname or a remote URL for the storage location of the DHCPv6 snooping database file.

The remaining statements are explained separately. See [CLI Explorer](#).

Default The IP-MAC bindings in the DHCPv6 snooping database are not persistent. If the switch is rebooted, the bindings are lost.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring Persistent Bindings in the DHCP or DHCPv6 \(ELS\) on page 381](#)
 - [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

dh-group

Syntax	<code>dh-group (group1 group2 group5 group14);</code>
Hierarchy Level	<code>[edit security ike proposal <i>ike-proposal-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the IKE Diffie-Hellman group.
Options	<p>dh-group—Type of Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. It can be one of the following:</p> <ul style="list-style-type: none"> • group1—768-bit. • group2—1024-bit. • group5—1536-bit. • group14—2048-bit.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the Diffie-Hellman Group for an IKE Proposal</i>

direction

Syntax	<code>direction (inbound outbound);</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Configure whether the secure channel applies MACsec security to traffic entering or leaving an interface.</p> <p>If you need to apply MACsec on traffic entering and leaving an interface, you need to create one secure channel to apply MACsec on incoming traffic and another secure channel to apply MACsec on outgoing traffic within the same connectivity association. When you associate the connectivity association with an interface, MACsec is applied on traffic entering and leaving that interface.</p> <p>You only use this configuration option when you are configuring MACsec using static secure association keys (SAK) security mode. When you are configuring MACsec using static connectivity association keys (CAK) security mode, two secure channels that are not user-configurable—one inbound secure channel and one outbound secure channel—are automatically created within the connectivity association.</p>
Default	<p>This statement does not have a default value.</p> <p>If you have configured a secure channel to enable MACsec using static SAK security mode, you must specify whether the secure channel applies MACsec to traffic entering or leaving an interface. A candidate configuration that contains a secure channel that has not configured a direction cannot be committed.</p>
Options	<p>inbound—Enable MACsec security on traffic entering the interface that has applied the secure channel.</p> <p>outbound—Enable MACsec security on traffic leaving the interface that has applied the secure channel.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

direction (Junos OS)

Syntax	<pre> direction (inbound outbound bidirectional) { authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text key hexadecimal key); } auxiliary-spi auxiliary-spi-value; encryption { algorithm (des-cbc 3des-cbc); key (ascii-text key hexadecimal key); } protocol (ah esp bundle); spi spi-value; } </pre>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the direction of IPsec processing.
Options	<p>inbound—Inbound SA—Define algorithms, keys, or security parameter index (SPI) values to decrypt and authenticate incoming traffic coming from the peer.</p> <p>outbound—Outbound SA—Define algorithms, keys, or SPI values to decrypt and authenticate outbound traffic to the peer.</p> <p>bidirectional—Bidirectional SA—Decrypt and authenticate the incoming and outgoing traffic using the same algorithm, keys, or SPI in both directions, unlike inbound and outbound SAs that use different attributes in both directions.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Manual IPsec Security Associations for an ES PIC on page 39 • <i>Example: Using IPsec to Protect BGP Traffic</i>

direction (Junos-FIPS Software)

Syntax	<pre>direction (bidirectional inbound outbound) { protocol esp; spi spi-value; encryption { algorithm 3des-cbc; key ascii-text <i>ascii-text-string</i>; } }</pre>
Hierarchy Level	[edit security ipsec internal security-association manual], [edit security trusted-channel ipsec security-association manual]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Establish a manual security association (SA) for internal Routing-Engine-to-Routing-Engine communication.
Options	bidirectional —Apply the same SA values in both directions between Routing Engines. inbound —Apply these SA properties only to the inbound IPsec tunnel. outbound —Apply these SA properties only to the outbound IPsec tunnel. The remaining statements are explained separately.
Required Privilege Level	Crypto Officer—To view and add this statement in the configuration.

direction (MX Series)

Syntax	<code>direction (inbound outbound);</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Configure whether the secure channel applies MACsec security to traffic entering or leaving an interface.</p> <p>If you need to apply MACsec on traffic entering and leaving an interface, you need to create one secure channel to apply MACsec on incoming traffic and another secure channel to apply MACsec on outgoing traffic within the same connectivity association. When you associate the connectivity association with an interface, MACsec is applied on traffic entering and leaving that interface.</p> <p>You only use this configuration option when you are configuring MACsec using static secure association keys (SAK) security mode. When you are configuring MACsec using static connectivity association keys (CAK) security mode, two secure channels that are not user-configurable—one inbound secure channel and one outbound secure channel—are automatically created within the connectivity association.</p>
Default	<p>This statement does not have a default value.</p> <p>If you have configured a secure channel to enable MACsec using static SAK security mode, you must specify whether the secure channel applies MACsec to traffic entering or leaving an interface. A candidate configuration that contains a secure channel that has not configured a direction cannot be committed.</p>
Options	<p>inbound—Enable MACsec security on traffic entering the interface that has applied the secure channel.</p> <p>outbound—Enable MACsec security on traffic leaving the interface that has applied the secure channel.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

disable-fpc (DDoS)

Syntax	disable-fpc;
Hierarchy Level	[edit system ddos-protection global], [edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)], [edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>) fpc <i>slot-number</i>]
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Support at the [edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)] hierarchy level introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.</p> <p>Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.</p>
Description	(MX Series routers with only MPCs, T4000 routers with only FPC5s, PTX Series routers, EX9200 switches, or QFX Series switches) Disable DDoS policers for debugging purposes on the card in the specified slot for a particular packet type within a protocol group, on all cards for a particular packet type within a protocol group, or globally on all cards and for all packet types in all protocols. This statement does not affect the state of the Routing Engine policers.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Disabling DDoS Protection Policers and Logging Globally on page 536• Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537

disable-logging (DDoS)

Syntax	<code>disable-logging;</code>
Hierarchy Level	<code>[edit system ddos-protection global],</code> <code>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]</code>
Release Information	Statement introduced in Junos OS Release 11.2. Support at the <code>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]</code> hierarchy level introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers. Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.
Description	(MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX Series switches) Disable device-wide logging of all DDoS violation and flow detection events globally. Disable only logging of events other than flow detection culprit flow events for a particular packet type or for a protocol group. Typically used for debugging purposes.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Disabling DDoS Protection Policers and Logging Globally on page 536 • Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537 • Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 574


disable-preceding-key

Syntax	disable-preceding-key;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 19.2R1 for MX Series routers.
Description	<p>Disable the preceding pre-shared key (PSK) so that the fallback PSK is used to establish a MACsec connection.</p> <p>When you enable MACsec using static CAK security mode, a preshared PSK is exchanged between the devices on each end of the point-to-point Ethernet link. The PSK must match across devices for a MACsec session to be established. If the primary PSK is changed on one device but not the other, the mismatch is resolved by using the older primary PSK. This is a temporary key known as the preceding PSK, and is not configurable.</p> <p>If a fallback PSK is configured, it will not take effect if the MACsec session is live with the preceding PSK. You can configure the disable-preceding-key statement so that the session switches to using the fallback PSK if there is a change to the primary PSK.</p>
Default	By default, the preceding PSK takes priority over the fallback PSK. Configure the disable-preceding-key to override this behavior.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec with Fallback PSK on page 279


disable-routing-engine (DDoS)

Syntax	<code>disable-routing-engine;</code>
Hierarchy Level	<code>[edit system ddos-protection global],</code> <code>[edit system ddos-protection protocols <i>protocol-group</i> (<i>aggregate</i> <i>packet-type</i>)</code>
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Disable DDoS Routing Engine policers for debugging purposes for a particular packet type within a protocol group or globally for all packet types in all protocols. This statement does not affect the state of the line card policers.
Required Privilege Level	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Disabling DDoS Protection Policers and Logging Globally on page 536

disable-timeout

Syntax	<code>disable-timeout <i>timeout</i>;</code>
Hierarchy Level	[edit ethernet-switching-options port-error-disable],
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches.
Description	Specify how long the Ethernet switching interfaces remain in a disabled state because of MAC limiting, MAC move limiting, or storm control errors.
	<div>  <p>NOTE: If you modify the timeout value of an existing disable timeout setting, the new timeout value does not impact the timing of restoration to service of currently disabled interfaces that have been configured for automatic recovery. The new timeout value is applied only during the next occurrence of a port error.</p> <p>You can bring up the currently disabled interfaces by running the operational command clear ethernet-switching port-error.</p> </div>
Default	The disable timeout is not enabled.
Options	<p>timeout—Time, in seconds, that the disabled state remains in effect. The disabled interface is automatically restored to service when the specified timeout value is reached.</p> <p>Range: 10 through 3600 seconds</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Autorecovery for Port Security Events on page 635 • Configuring Autorecovery for Port Security Events on page 635

disable-timeout (Port Error Disable)

Syntax	<code>disable-timeout <i>timeout</i>;</code>
Hierarchy Level	[edit ethernet-switching-options port-error-disable]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Specify how long Ethernet switching interfaces remain in a disabled state due to MAC limiting, MAC move limiting, or storm control errors.
	<div>  <p>NOTE: If you modify an existing timeout value, the new timeout value does not affect currently disabled interfaces are configured for automatic recovery. The new timeout value applies only to subsequent port errors. Run the <code>clear ethernet-switching port-error</code> command to restore currently disabled interfaces.</p> </div>
Default	The disable timeout statement is not enabled.
Options	<p><i>timeout</i>—Time, in seconds, that an interface remains disabled. The disabled interface automatically returns to service when the specified time expires.</p> <p>Range: 10 through 3600 seconds</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding MAC Limiting and MAC Move Limiting for Port Security • Understanding Storm Control on page 622 • Example: Using Storm Control to Prevent Network Outages (non-ELS) on page 638 • Example: Using Storm Control to Prevent Network Outages on page 636 • action-shutdown

discard

Syntax	<pre>discard { prefix-list-name <i>prefix-list-name</i>; source-ip-address-list <i>address-list-name</i>; source-mac-address-list <i>address-list-name</i>; }</pre>
Hierarchy Level	[edit forwarding-options access-security router-advertisement-guard <i>policy</i> <i>policy-name</i>]
Release Information	<p>Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.</p> <p>Statement introduced in Junos OS Release 16.1 for EX Series switches.</p>
Description	<p>Configure a discard policy for an IPv6 Router Advertisement (RA) guard policy. RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in the policy.</p> <p>When RA guard is enabled, the switch compares the information contained in the attributes of RA messages to the criteria configured in the policy. When RA guard is enabled by using a discard policy, any RA messages that match the conditions defined in the policy are dropped, and RA messages that do not match the conditions are forwarded.</p> <p>The criteria are configured as one or more lists of IPv6 addresses, MAC addresses, or IPv6 address prefixes associated with the policy. RA guard compares the source address or address prefix of incoming RA messages with the configured lists. You configure the lists at the [edit policy-options] hierarchy level, by using the prefix-list option for an IPv6 address or address prefix list, and the mac-list option for a MAC address list.</p> <p>If more than one list is associated with a discard policy, then an incoming RA message that meets the criteria in any of the lists is discarded.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514

dynamic

Syntax	<pre>dynamic { ipsec-policy <i>ipsec-policy-name</i>; replay-window-size (32 64); }</pre>
Hierarchy Level	[edit security ipsec security-association name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define a dynamic IPsec SA.
Options	<p>ipsec-policy <i>ipsec-policy-name</i>—Name of the IPsec policy.</p> <p>replay-window-size—(Optional) Antireplay window size. It can be one of the following values:</p> <ul style="list-style-type: none"> • 32—32-packet window size. • 64—64-packet window size.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Dynamic IPsec Security Associations on page 43 • Associating the Configured Security Association with a Logical Interface on page 184

encoding

Syntax	encoding (binary pem);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>], [edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file format used for the local-certificate and local-key-pair statements.
Options	binary —Binary file format. pem —Privacy-enhanced mail (PEM), an ASCII base 64 encoded format. Default: binary
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Type of Encoding Your CA Supports on page 179• Configuring an IKE Policy for Digital Certificates for an ES PIC on page 182



encryption (MACsec)

Syntax	encryption;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Enable MACsec encryption within a secure channel.</p> <p>You can enable MACsec without enabling encryption. If a connectivity association with a secure channel that has not enabled MACsec encryption is associated with an interface, traffic is forwarded across the Ethernet link in clear text. You are, therefore, able to view this unencrypted traffic when you are monitoring the link. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic has not been tampered with and does not represent a security threat.</p> <p>Traffic traversing a MAC-enabled point-to-point Ethernet link traverses the link at the same speed regardless of whether encryption is enabled or disabled. You cannot increase the speed of traffic traversing a MACsec-enabled Ethernet link by disabling encryption.</p> <p>This command is used to enable encryption when MACsec is configured using secure association key (SAK) security mode only. When MACsec is configuring using static connectivity association key (CAK) security mode, the encryption setting is configured outside of the secure channel using the no-encryption configuration statement.</p>
Default	MACsec encryption is disabled when MACsec is configured using static SAK security mode, by default.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

encryption (MACsec for MX Series)

Syntax	encryption;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Enable MACsec encryption within a secure channel.</p> <p>You can enable MACsec without enabling encryption. If a connectivity association with a secure channel that has not enabled MACsec encryption is associated with an interface, traffic is forwarded across the Ethernet link in clear text. You are, therefore, able to view this unencrypted traffic when you are monitoring the link. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic has not been tampered with and does not represent a security threat.</p> <p>Traffic traversing a MAC-enabled point-to-point Ethernet link traverses the link at the same speed regardless of whether encryption is enabled or disabled. You cannot increase the speed of traffic traversing a MACsec-enabled Ethernet link by disabling encryption.</p> <p>This command is used to enable encryption when MACsec is configured using secure association key (SAK) security mode only. When MACsec is configuring using static connectivity association key (CAK) security mode, the encryption setting is configured outside of the secure channel using the no-encryption configuration statement.</p>
Default	MACsec encryption is disabled when MACsec is configured using static SAK security mode, by default.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

encryption (Junos OS)

Syntax	<pre> encryption { algorithm (des-cbc 3des-cbc aes-128-cbc aes-192-cbc aes-256-cbc); key (ascii-text key hexadecimal key); } </pre>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bidirectional)]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>aes-128-cbc, aes-192-cbc, and aes-256-cbc algorithm options added in Junos OS Release 15.1.</p>
Description	Configure an encryption algorithm and key for a manual Security Association.
Options	<p>algorithm—Type of encryption algorithm. It can be one of the following:</p> <ul style="list-style-type: none"> • des-cbc—Has a block size of 8 bytes (64 bits); its key size is 48 bits long. • 3des-cbc—Has block size of 8 bytes (64 bits); its key size is 192 bits long. <p> NOTE: For 3des-cbc, we recommend that the first 8 bytes be different from the second 8 bytes, and the second 8 bytes be the same as the third 8 bytes.</p> <ul style="list-style-type: none"> • aes-128-cbc—Has a block size of 128 bits; its key size is 128 bits long. • aes-192-cbc—Has a block size of 128 bits; its key size is 192 bits long. • aes-256-cbc—Has a block size of 128 bits; its key size is 256 bits long. <p> NOTE: The aes-*-cbc algorithms support both IKE and IPsec configurations at the [security] hierarchy level.</p> <p>key—Type of encryption key. It can be one of the following:</p> <ul style="list-style-type: none"> • ascii-text—ASCII text key. For the des-cbc option, the key contains 8 ASCII characters; for 3des-cbc, the key contains 24 ASCII characters. • hexadecimal—Hexadecimal key. For the des-cbc option, the key contains 16 hexadecimal characters; for the 3des-cbc option, the key contains 48 hexadecimal characters.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Example: Using IPsec to Protect BGP Traffic](#)
- [Configuring Manual IPsec Security Associations for an ES PIC on page 39](#)

encryption (Junos-FIPS Software)

Syntax

```
encryption {  
  algorithm 3des-cbc;  
  key ascii-text ascii-text-string;  
}
```

Hierarchy Level [edit security ipsec internal security-association manual direction]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the encryption parameters for internal Routing-Engine-to-Routing-Engine communication. The remaining statements are explained separately.



NOTE: The hexadecimal format must be used for the encryption key to be FIPS compliant. The hexadecimal keys provide maximum key strength.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

encryption-algorithm (Security)

Syntax	encryption-algorithm (3des-cbc des-cbc aes-128-cbc aes-192-cbc aes-256-cbc);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure an IKE or IPsec encryption algorithm.
Options	<p>3des-cbc—Encryption algorithm with key size of 24 bytes; its key size is 192 bits long.</p> <p>des-cbc—Encryption algorithm with key size of 8 bytes; its key size is 48 bits long.</p> <p>aes-128-cbc—Advanced encryption algorithm that has a key size of 16 bytes; its key size is 128 bits long.</p> <p>aes-192-cbc—Advanced encryption algorithm that has a key size of 24 bytes; its key size is 192 bits long.</p> <p>aes-256-cbc—Advanced encryption algorithm that has a key size of 32 bytes; its key size is 256 bits long.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Proposal for Dynamic SAs • Configuring an IPsec Proposal for an ES PIC

enrollment

Syntax	<pre>enrollment { url <i>url-name</i>; retry <i>number-of-enrollment-attempts</i>; retry-interval <i>seconds</i>; }</pre>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	Specify the URL and enrollment parameters of the certificate authority (CA) for Adaptive Services (AS) and MultiServices PICs installed on MX Series, M Series, and T Series routers.
Options	<p>url <i>url-name</i>—Location of the CA to which the router sends the Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests for the configured CA profile. Use the CA host DNS name or IP address.</p> <p>retry <i>number-of-enrollment-attempts</i>—Number of enrollment retries. Range: 0 through 100 Default: 0</p> <p>retry-interval <i>seconds</i>—Length of time, in seconds, that a router should wait between enrollment attempts. Range: 0 through 3600 Default: 0</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying an Enrollment URL on page 187• Specifying the Enrollment Properties on page 187

enrollment-retry

Syntax	<code>enrollment-retry <i>attempts</i>;</code>
Hierarchy Level	<code>[edit security certificates]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify how many times a router or switch can resend a digital certificate request.
Options	<i>attempts</i> —Number of enrollment retries. Range: 0 through 100 Default: 0
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Number of Enrollment Retries on page 180

enrollment-url

Syntax	<code>enrollment-url <i>url-name</i>;</code>
Hierarchy Level	<code>[edit security certificates certification-authority <i>ca-profile-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify where your router or switch sends Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).
Options	<i>url-name</i> —Certificate authority URL.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying an Enrollment URL on page 179

ethernet-switching-options

List of Syntax [EX Series on page 755](#)
 [QFX Series, QFabric, EX4600 on page 758](#)

```

EX Series ethernet-switching-options {
    analyzer (Port Mirroring) {
        name {
            loss-priority priority;
            ratio number;
            input {
                ingress {
                    interface (all | interface-name);
                    vlan (vlan-id | vlan-name);
                }
                egress {
                    interface (all | interface-name);
                }
            }
            output {
                interface interface-name;
                vlan (vlan-id | vlan-name) {
                    no-tag;
                }
            }
        }
    }
    bpdv-block {
        disable-timeout timeout;
        interface (all | [interface-name]) {
            (disable | drop | shutdown);
        }
    }
    dot1q-tunneling {
        ether-type (0x8100 | 0x88a8 | 0x9100);
    }
    interfaces interface-name {
        no-mac-learning;
    }
    mac-lookup-length number-of-entries;
}
    mac-notification {
        notification-interval seconds;
    }
    mac-table-aging-time seconds;
    nonstop-bridging;
    port-error-disable {
        disable-timeout timeout;
    }
    redundant-trunk-group {
        group name {
            interface interface-name <primary>;
            interface interface-name;
        }
    }
}

```

```

    }
  }
  secure-access-port {
    dhcp-snooping-file {
      location local_pathname | remote_URL;
      timeout seconds;
      write-interval seconds;
    }
    dhcpv6-snooping-file {
      location local_pathname | remote_URL;
      timeout seconds;
      write-interval seconds;
    }
  }
  interface (all | interface-name) {
    allowed-mac {
      mac-address-list;
    }
    (dhcp-trusted | no-dhcp-trusted);
    fcoe-trusted;
    mac-limit limit action (drop | log | none | shutdown);
    no-allowed-mac-log;
    persistent-learning;
    static-ip ip-address {
      vlan vlan-name;
      mac mac-address;
    }
    static-ipv6 ip-address {
      vlan vlan-name;
      mac mac-address;
    }
  }
  vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection) [
      forwarding-class class-name;
    ]
    dhcp-option82 {
      circuit-id {
        prefix hostname;
        use-interface-description;
        use-vlan-id;
      }
      remote-id {
        prefix hostname | mac | none;
        use-interface-description;
        use-string string;
      }
      vendor-id [string];
    }
    (examine-dhcp | no-examine-dhcp) {
      forwarding-class class-name;
    }
    (examine-dhcpv6 | no-examine-dhcpv6) {
      forwarding-class class-name;
    }
    examine-fip {

```



```

    fc-map fc-map-value;
  }
  (ip-source-guard | no-ip-source-guard);
  (ipv6-source-guard | no-ipv6-source-guard);
  mac-move-limit limit action (drop | log | none | shutdown);
  }
  (neighbor-discovery-inspection | no-neighbor-discovery-inspection);
no-option-37;
static {
  vlan name {
    mac mac-address {
      next-hop interface-name;
    }
  }
}
storm-control {
  action-shutdown;
  interface (all | interface-name) {
    bandwidth bandwidth;
    level level;
    multicast;
    no-broadcast;
    no-multicast;
    no-registered-multicast;
    no-unknown-unicast;
    no-unregistered-multicast;
  }
}
traceoptions {
  file filename <files number> <no-stamp> <replace> <size size> <world-readable |
    no-world-readable>;
  flag flag <disable>;
}
unknown-unicast-forwarding {
  vlan (all | vlan-name) {
    interface interface-name;
  }
}
}
voip {
  interface (all | [interface-name | access-ports]) {
    vlan vlan-name;
    forwarding-class (assured-forwarding | best-effort | expedited-forwarding |
      network-control);
  }
}
}
}

```

QFX Series, QFabric,
EX4600

```

ethernet-switching-options {
  analyzer {
    name {
      input {
        egress {
          interface (all | interface-name);
        }
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
      }
      output {
        interface interface-name;
        ip-address ip-address;
        vlan (vlan-id | vlan-name);
      }
    }
  }
  bpdu-block {
    interface (all | [interface-name]);
    disable-timeout timeout;
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100)
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-table-aging-time seconds {
  }
  port-error-disable {
    disable-timeout timeout;
  }
  secure-access-port {
    dhcp-snooping-file {
      location local_pathname | remote_URL;
      timeout seconds;
      write-interval seconds;
    }
    interface (all | interface-name) {
      allowed-mac {
        mac-address-list;
      }
      (dhcp-trusted | no-dhcp-trusted);
      fcoe-trusted;
      mac-limit limit action action;
      no-allowed-mac-log;
    }
    vlan (all | vlan-name) {
      (arp-inspection | no-arp-inspection) [
        forwarding-class (for DHCP Snooping or DAI Packets) class-name;
      ]
      dhcp-option82 {
        circuit-id {
          prefix (Circuit ID for Option 82) hostname;
        }
      }
    }
  }
}

```

```

    use-interface-description;
    use-vlan-id;
  }
  remote-id {
    prefix (Remote ID for Option 82) hostname | mac | none;
    use-interface-description;
    use-string string;
  }
  vendor-id <string>;
}
(examine-dhcp | no-examine-dhcp) {
  forwarding-class (for DHCP Snooping or DAI Packets) class-name;
}
examine-fip {
  examine-vn2vn {
    beacon-period milliseconds;
  }
  fc-map fc-map-value;
}
mac-move-limit limit <fabric-limit limit action action>;
}
}
static {
  vlan vlan-id {
    mac mac-address next-hop interface-name;
  }
}
storm-control {
  interface (all | interface-name) {
    bandwidth bandwidth;
    no-broadcast;
    no-multicast;
    no-unknown-unicast;
  }
}
traceoptions {
  file filename <files number> <no-stamp> <replace> <size size> <world-readable |
  no-world-readable>;
  flag flag <disable>;
}
}

```

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

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure Ethernet switching options.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Understanding Port Mirroring</i>• Understanding How to Protect Access Ports from Common Attacks on page 6• Port Security Features on page 3• <i>Understanding BPDU Protection for STP, RSTP, and MSTP</i>• <i>Understanding Redundant Trunk Links (Legacy RTG Configuration)</i>• Understanding Storm Control on page 622• <i>Understanding 802.1X and VoIP on EX Series Switches</i>• <i>Understanding Q-in-Q Tunneling and VLAN Translation</i>• Understanding and Preventing Unknown Unicast Forwarding on page 613• <i>Understanding MAC Notification on EX Series Switches</i>• <i>Understanding FIP Snooping</i>• <i>Understanding Nonstop Bridging on EX Series Switches</i>

examine-dhcp

Syntax `(examine-dhcp | no-examine-dhcp) {
 forwarding-class class-name;
}`

Hierarchy Level `[edit ethernet-switching-options secure-access-port vlan (all | vlan-name)]`

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Enable DHCP snooping on all VLANs or on the specified VLAN.



NOTE: If you configure DHCP for all VLANs and you enable a different port security feature on a specific VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.

- **examine-dhcp**—Enable DHCP snooping.
- **no-examine-dhcp**—Disable DHCP snooping.

When DHCP snooping is enabled, the switch logs DHCP packets (DHCP OFFER, DHCP DECLINE, DHCP ACK, and DHCP NAK packets) that it receives on untrusted ports. You can monitor the log for these messages, which can signal the presence of a malicious DHCP server on the network.



TIP: For private VLANs (PVLANS), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from PVLAN trunk ports are not snooped.

The remaining statement is explained separately.

Default Disabled.



Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks on page 406](#)
- [Example: Protecting Against ARP Spoofing Attacks on page 418](#)


- [Example: Prioritizing Snooped and Inspected Packet on page 423](#)
- [Enabling DHCP Snooping \(non-ELS\) on page 400](#)
- *Enabling DHCP Snooping (J-Web Procedure)*

examine-dhcpv6

Syntax	<pre>examine-dhcpv6 { forwarding-class class-name; }</pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	<p>Enable DHCPv6 snooping on all VLANs or on the specified VLAN.</p> <p> NOTE: If you configure DHCP for all VLANs and you enable a different port security feature on a specific VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to that VLAN.</p> <p>When DHCP snooping is enabled, the switch logs DHCP packets (DHCP OFFER, DHCP DECLINE, DHCP ACK, and DHCP NAK packets) that it receives on untrusted ports. You can monitor the log for these messages, which can signal the presence of a malicious DHCP server on the network.</p> <p> TIP: For private VLANs (PVLANS), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from PVLAN trunk ports are not snooped.</p> <p>The remaining statement is explained separately.</p>
Default	Disabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Port Security (non-ELS) on page 15 • Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks on page 406 • Example: Protecting Against ARP Spoofing Attacks on page 418 • Example: Prioritizing Snooped and Inspected Packet on page 423 • Enabling DHCP Snooping (non-ELS) on page 400

- *Enabling DHCP Snooping (J-Web Procedure)*

examine-fip

Syntax	<pre>examine-fip { examine-vn2vn { beacon-period <i>milliseconds</i>; } fc-map <i>fc-map-value</i>; no-fip-snooping-scaling; }</pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>)]
Release Information	<p>Statement introduced in Junos OS Release 10.4 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement examine-vn2vn introduced in Junos OS Release 12.2 for the QFX Series.</p> <p>Statement no-fip-snooping-scaling introduced in Junos OS Release 13.2X52-D10 for the QFX Series.</p>
Description	<p> NOTE: This statement supports the original CLI. If your switch runs the Enhanced Layer 2 Software (ELS) CLI, see <i>examine-vn2vf</i> for VN_Port to VF_Port (VN2VF_Port) FIP snooping, and see <i>examine-vn2vn</i> for VN_Port to VN_Port (VN2VN_Port) FIP snooping. For ELS details, see <i>Using the Enhanced Layer 2 Software CLI</i>.</p> <p>Enable FIP snooping on a specified VLAN. Ensure that the VLAN is a dedicated FCoE VLAN that transports only FCoE traffic.</p> <p>(QFX Series only) Enable VN2VN_Port FIP snooping on the specified VLAN. The VLAN must be a dedicated FCoE VLAN that transports only VN2VN_Port traffic. One FCoE VLAN cannot support both VN2VF_Port FIP snooping and VN2VN_Port FIP snooping. Configure separate, dedicated FCoE VLANs for VN2VN_Port FIP snooping and VN2VN_Port FIP snooping.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • vlan on page 1058 • <i>Example: Configuring an FCoE Transit Switch</i> • <i>Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch</i>

exclude-protocol

Syntax	<code>exclude-protocol <i>protocol-name</i>;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specifies protocols whose packets are not secured using Media Access Control Security (MACsec) when MACsec is enabled on a link using static connectivity association key (CAK) security mode.</p> <p>When this option is enabled in a connectivity association that is attached to an interface, MACsec is not enabled for all packets of the specified protocols that are sent and received on the link.</p>
Default	<p>Disabled.</p> <p>All packets are secured on a link when MACsec is enabled, with the exception of all types of Spanning Tree Protocol (STP) packets.</p>
Options	<p><i>protocol-name</i>—Specifies the name of the protocol that should not be MACsec-secured. Options include:</p> <ul style="list-style-type: none">• cdp—Cisco Discovery Protocol.• lcp—Link Aggregation Control Protocol.• lldp—Link Level Discovery Protocol.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228

exclude-protocol (MX Series)

Syntax	<code>exclude-protocol <i>protocol-name</i>;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specifies protocols whose packets are not secured using Media Access Control Security (MACsec) when MACsec is enabled on a link using static connectivity association key (CAK) security mode.</p> <p>When this option is enabled in a connectivity association that is attached to an interface, MACsec is not enabled for all packets of the specified protocols that are sent and received on the link.</p>
Default	<p>Disabled.</p> <p>All packets are secured on a link when MACsec is enabled, with the exception of all types of Spanning Tree Protocol (STP) packets.</p>
Options	<p><i>protocol-name</i>—Specifies the name of the protocol that should not be MACsec-secured. Options include:</p> <ul style="list-style-type: none"> • cdp—Cisco Discovery Protocol. • lcp—Link Aggregation Control Protocol. • lldp—Link Level Discovery Protocol.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

fallback-key

Syntax	<pre>fallback-key { cak hexadecimal-number; ckn hexadecimal-number; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 19.2R1 for MX Series routers.
Description	<p>Specifies the fallback preshared key (PSK) to be used to enable MACsec using static connectivity association key (CAK) security mode. You can configure a fallback PSK to prevent traffic loss in case the primary PSK fails to establish a connection.</p> <p>When you enable MACsec using static CAK security mode, a preshared PSK is exchanged between the devices on each end of the point-to-point Ethernet link. The PSK includes a connectivity association name (CKN) and a connectivity association key (CAK). The PSK must match across devices for a MACsec session to be established. If there is a mismatch, the session will not be established and all packets will be dropped. The fallback PSK is used when the primary PSK does not match for the initial MACsec negotiation.</p>
Default	Fallback PSK is not enabled by default.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec with Fallback PSK on page 279

family vpls (Layer 2 Pseudowires)

Syntax	family vpls;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	Specify that the protocol family for the logical interface is VPLS.
Required Privilege Level	router—To view this statement in the configuration. router-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Applying the Policers to Dynamic Profile Interfaces</i>• <i>Creating a Dynamic Profile for the Complex Configuration</i>

fc-map

Syntax `fc-map fc-map-value;`

Hierarchy Level Original CLI

[edit ethernet-switching options secure-access-port vlan (all | *vlan-name*) **examine-fip**]

ELS CLI for Platforms that Support FCoE

[edit vlans *vlan-name* forwarding-options fip-security]



NOTE: The `fc-map` configuration statement is in a different hierarchy on the original CLI than on the Enhanced Layer 2 Software (ELS) CLI.

QFX Series that Support FCoE-FC Gateway Configuration

[edit fc-fabrics *fc-fabric-name* protocols fip]

Release Information Statement introduced in Junos OS Release 10.4 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced for the ELS CLI in Junos OS Release 13.2 for the QFX Series.

Description Set the FCoE mapped address prefix (FC-MAP) value for the FCoE VLAN to match the FC switch (or FCoE forwarder) FC-MAP value for the FC fabric. The FC-MAP value is a unique MAC address prefix an FC switch uses to identify FCoE traffic for a given FC fabric (traffic on a particular FCoE VLAN).

You can configure the FC-MAP value or use the default value. The default FC-MAP value is different for VN_Port to VF_Port (VN2VF_Port) FIP snooping (0x0EFC00) than for VN_Port to VN_Port (VN2VN_Port) FIP snooping.

The FC switch provides the FC-MAP value to FCoE nodes (ENodes) in the FIP discovery advertisement message. If the EX Series switch or the QFX Series FCoE VLAN FC-MAP value does not match the FC switch FC-MAP value, neither device discovers the FC switch on that VLAN, and the ENodes on that VLAN cannot access the FC switch. The FC switch accepts only FCoE traffic that uses the correct FC-MAP value as part of the VN_Port MAC address.


When the QFX Series acts as an FCoE-FC gateway, the FC-MAP value for the gateway and the FCoE devices must match the FC switch FC-MAP value in order to communicate with the FC switch.



NOTE: Changing the FC-MAP value causes all logins to drop and forces the ENodes to log in again.

Options	<i>fc-map-value</i> —FC-MAP value, hexadecimal value preceded by “0x”. Range: 0x0EFC00 through 0x0EFCFF Default: 0x0EFC00 for VN2VF_Port FIP snooping 0x0EFD00 for VN2VN_Port FIP snooping
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• examine-fip on page 765• <i>show fip snooping</i>• <i>Example: Configuring an FCoE Transit Switch</i>• <i>Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch</i>

fcoe-trusted

Syntax	fcoe-trusted;
Hierarchy Level	Original CLI <pre>[edit ethernet-switching-options secure-access-port interface <i>interface-name</i>]</pre> <p>ELS CLI for Platforms that Support FCoE</p> <pre>[edit vlans <i>vlan-name</i> forwarding-options fip-security interface <i>interface-name</i>]</pre> <p>.....</p> <p> NOTE: The fcoe-trusted configuration statement is in a different hierarchy on the original CLI than on the Enhanced Layer 2 Software (ELS) CLI.</p> <p>.....</p> <p>QFX Series that Support FCoE-FC Gateway Configuration</p> <pre>[edit fc-fabrics <i>fc-fabric-name</i> protocols fip]</pre>
Release Information	Statement introduced in Junos OS Release 10.4 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced for the FC fabric in Junos OS Release 11.3 for the QFX Series. Statement introduced for the ELS CLI in Junos OS Release 13.2 for the QFX Series.
Description	Configure the specified 10-Gigabit Ethernet interface to trust Fibre Channel over Ethernet (FCoE) traffic. If an interface is connected to another switch such as an FCoE forwarder (FCF) or a transit switch, you can configure the interface as trusted so that the interface forwards FCoE traffic from the switch to the FCoE devices without installing FIP snooping filters.
	(QFX Series FCoE-FC gateway) Configure the specified local Fibre Channel fabric to trust FCoE traffic on all ports in the fabric. Changing the fabric ports from untrusted to trusted removes any existing FIP snooping filters from the ports. Changing the fabric ports from trusted to untrusted by removing the fcoe-trusted configuration from the fabric forces all of the FCoE sessions on those ports to log out so that when the ENodes and VN_Ports log in again, the switch can build the appropriate FIP snooping filters.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> <i>show fip snooping</i> <i>Example: Configuring an FCoE Transit Switch</i>

- *Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*
- *Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

file

Syntax	<code>file <i>certificate-filename</i>;</code>
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file from which to read the digital certificate.
Options	<i>certificate-filename</i> —File from which to read the digital certificate.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Specifying a File to Read the Digital Certificate on page 179

flood (VLANs)

Syntax	<pre>flood { input <i>filter-name</i>; }</pre>
Hierarchy Level	<pre>[edit vlans <i>vlan-name</i>], [edit vlans <i>vlan-name</i> forwarding-options]</pre>
Release Information	Statement introduced in Junos OS Release 14.2 for EX Series switches.
Description	<p>Apply a flood filter to traffic ingressing a VLAN. Flood filters are triggered only for broadcast, unknown unicast, and multicast (BUM) traffic.</p> <p>Flood filters and firewall filters can coexist on the same VLAN. If the actions in the filters are conflicting, then the firewall filter takes priority over the flood filter.</p>
Default	All incoming traffic is accepted unmodified to a VLAN, and all outgoing traffic is sent unmodified from a VLAN.
Options	<p><i>filter-name</i>—Name of a filter defined at the <code>[edit firewall family <i>family-name</i> filter]</code> hierarchy level.</p> <p><i>input</i>—Apply a flood filter to VLAN ingress traffic.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Unknown Unicast Forwarding (ELS) on page 614• Configuring Firewall Filters• Overview of Firewall Filters

flow-detection (DDoS Flow Detection)

Syntax	<code>flow-detection;</code>
Hierarchy Level	<code>[edit system ddos-protection global]</code>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	<p>(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Enable flow detection globally for all protocol groups and packet types except the following, which do not have typical Ethernet, IP, or IPv6 headers:</p> <ul style="list-style-type: none"> Protocol groups: fab-probe, frame-relay, inline-ka, isis, jfm, mlp, pfe-alive, pos, and services. Packet type: unclassified in the ip-options protocol group.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Enabling Flow Detection for All Protocol Groups and Packet Types on page 573 <i>Configuring Flow Detection for DDoS Protection</i>


flow-detection (DDoS Packet Level)

Syntax	<pre> flow-detection { flow-detect-time detect-period; no-flow-logging; timeout-active-flows enable-period; flow-level-bandwidth { logical-interface flow-bandwidth; physical-interface flow-bandwidth; subscriber flow-bandwidth; } flow-level-control { logical-interface flow-control-mode; physical-interface flow-control-mode; subscriber flow-control-mode; } flow-level-detection { logical-interface operation-mode; physical-interface operation-mode; subscriber operation-mode; } flow-detection-mode (automatic off on); flow-recover-time recover-period; flow-timeout-time timeout-period; } </pre>
Hierarchy Level	[edit system ddos-protection protocols protocol-group packet-type]
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p>
Description	<p>(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure DDoS protection suspicious control flow detection for a packet type.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <i>Configuring Flow Detection for DDoS Protection</i>


flow-detection-mode (DDoS Flow Detection)

Syntax	<code>flow-detection-mode (automatic off on)</code>
Hierarchy Level	<code>[edit system ddos-protection protocols protocol-group packet-type]</code>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure the mode of operation for flow detection for a protocol group or packet type. Use this statement to override global flow detection settings configured with the flow-detection-mode statement at the <code>[edit system ddos-protection global]</code> hierarchy level. The operation mode is effective only when flow detection is enabled.
Default	The default mode for all protocol groups and packet types is automatic .
Options	<p>automatic—Detect flows only when the policer is being violated.</p> <p>off—Disable flow detection.</p> <p>on—Always monitor and detect flows, even when the policer is not being violated.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <i>Configuring How Flow Detection Operates for Individual Protocol Groups or Packets</i> <i>Configuring Flow Detection for DDoS Protection</i>

flow-detection-mode (DDoS Global Flow Detection)

Syntax	flow-detection-mode (automatic off on)
Hierarchy Level	[edit system ddos-protection global]
Release Information	Statement introduced in Junos OS Release 17.1.
Description	<p>(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure the mode of operation for flow detection globally for almost all protocol groups and packet types. The operation mode is effective only when flow detection is enabled.</p> <p> NOTE: You cannot enable flow detection globally for the following groups and packet type because they do not have typical Ethernet, IP, or IPv6 headers:</p> <ul style="list-style-type: none"> Protocol groups: fab-probe, frame-relay, inline-ka, isis, jfm, mlp, pfe-alive, pos, and services. Packet type: unclassified in the ip-options protocol group. <p>To override the global configuration for a protocol group or packet type, use the flow-detection-mode statement at the [edit system ddos-protection protocols protocol-group packet-type] hierarchy level.</p>
Default	The default global mode is automatic .
Options	<p>automatic—Detect flows only when the policer is being violated.</p> <p>off—Disable flow detection.</p> <p>on—Always monitor and detect flows, even when the policer is not being violated.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <i>Configuring How Flow Detection Operates for Individual Protocol Groups or Packets</i> <i>Configuring Flow Detection for DDoS Protection</i>

flow-detect-time (DDoS Flow Detection)

Syntax	<code>flow-detect-time <i>seconds</i>;</code>
Hierarchy Level	<code>[edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-detection]</code>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure how much time must pass before a suspicious flow that has exceeded the bandwidth allowed for the packet type is confirmed to be a culprit flow.
	<div>  <p>BEST PRACTICE: We recommend that you use the default value for the detection period.</p> </div>
Options	<p><i>seconds</i>—Period of excessive bandwidth required for flow to be a culprit flow.</p> <p>Range: 1 through 60 seconds</p> <p>Default: 3 seconds</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Detection Period for Suspicious Flows on page 569 • Configuring Flow Detection for DDoS Protection

flow-level-bandwidth (DDoS Flow Detection)

Syntax	<pre>flow-level-bandwidth { logical-interface <i>flow-bandwidth</i>; physical-interface <i>flow-bandwidth</i>; subscriber <i>flow-bandwidth</i>; }</pre>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i>]
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	<p>(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure allowed flow bandwidth for the packet type at each flow aggregation level.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 575• <i>Configuring Flow Detection for DDoS Protection</i>


flow-level-control (DDoS Flow Detection)

Syntax	<pre> flow-level-control { logical-interface flow-control-mode; physical-interface flow-control-mode; subscriber flow-control-mode; } </pre>
Hierarchy Level	[edit system ddos-protection protocols protocol-group packet-type]
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	<p>(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Specify how traffic in the detected flow is handled for the protocol group or packet type at one or more flow aggregation levels. Use this statement to override global flow control mode settings configured with the flow-level-control statement at the [edit system ddos-protection global] hierarchy level.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 572 • <i>Configuring Flow Detection for DDoS Protection</i>

flow-level-control (DDoS Global Flow Detection)

Syntax	<code>flow-level-control <i>flow-control-mode</i>;</code>
Hierarchy Level	<code>[edit system ddos-protection global]</code>
Release Information	Statement introduced in Junos OS Release 17.1.
Description	<p>(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Specify how traffic in the detected flow is handled globally for all protocol groups and packet types at all flow aggregation levels.</p> <p>To override the global configuration for a protocol group or packet type, use the flow-level-control statement at the <code>[edit system ddos-protection protocols <i>protocol-group packet-type</i>]</code> hierarchy level to specify the flow control mode at one or more flow aggregation levels.</p>
Options	<p><i>flow-control-mode</i>—Mode for how traffic in the detected flow is controlled globally.</p> <ul style="list-style-type: none">• drop—Drop all traffic in flow.• keep—Keep all traffic in flow.• police—Police the traffic to within its allowed bandwidth. <p>Default: drop</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring How Traffic in a Culprit Flow Is Controlled Globally on page 578• Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 572• Configuring Flow Detection for DDoS Protection

flow-level-detection (DDoS Flow Detection)

Syntax	<pre> flow-level-detection { logical-interface <i>flow-detection-mode</i>; physical-interface <i>flow-detection-mode</i>; subscriber <i>flow-detection-mode</i>; } </pre>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i>]
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	<p>(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure the mode of operation for flow detection for the packet type at each flow aggregation level.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
<div style="display: flex; align-items: center;">  <div> <p>NOTE: Flow detection operates for individual flow aggregation levels only when the flow detection mode at the packet level is configured to either automatic or on.</p> </div> </div>	
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 571 • Configuring Flow Detection for DDoS Protection

flow-recover-time (DDoS Flow Detection)

Syntax	<code>flow-recover-time <i>seconds</i>;</code>
Hierarchy Level	<code>[edit system ddos-protection protocols <i>protocol-group packet-type</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	<p>(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure how much time must pass before a culprit flow for the packet type is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation.</p>
Options	<p><i>seconds</i>—Period required for the traffic to recover.</p> <p>Range: 1 through 3600 seconds</p> <p>Default: 60 seconds</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Recovery Period for a Culprit Flow on page 569• Configuring Flow Detection for DDoS Protection


flow-report-rate (DDoS Flow Detection)

Syntax	<code>flow-report-rate <i>report-rate</i>;</code>
Hierarchy Level	<code>[edit system ddos-protection global]</code>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Set the rate at which culprit flow events are reported by system log messages, for all protocol groups and packet types on all line cards.
Options	<p><i>report-rate</i>—Number of flows per second.</p> <p>Range: 1 through 50,000</p> <p>Default: 10</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types on page 574 • <i>Configuring Flow Detection for DDoS Protection</i>

flow-timeout-time (DDoS Flow Detection)

Syntax	<code>flow-timeout-time seconds;</code>
Hierarchy Level	<code>[edit system ddos-protection protocols <i>protocol-group packet-type</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	<p>(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure the period of time that a culprit flow is suppressed for the packet type. The timeout period is effective only when timing out has been enabled with the timeout-active-flows statement.</p>
Options	<p>seconds—Period that the traffic is suppressed.</p> <p>Range: 1 through 7200 seconds</p> <p>Default: 300 seconds</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Timeout Period for a Culprit Flow on page 570• Configuring Flow Detection for DDoS Protection

forwarding-class (for DHCP Snooping or DAI Packets)

Syntax	<code>forwarding-class class <i>class-name</i>;</code>
Hierarchy Level	[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>) (examine-dhcp arp-inspection)]
Release Information	Statement introduced in Junos OS Release 11.2 for EX Series switches. Statement introduced in Junos OS Release 12.1 for the QFX Series.
Description	Assign a user-defined or a predefined forwarding class to the packets that have been checked for DHCP snooping or dynamic ARP inspection (DAI).
	<div>  <p>NOTE: To assign a user-defined class, you must first configure the user-defined class by using the <i>forwarding-classes</i> configuration statement at the [edit <i>class-of-service</i>] hierarchy level.</p> </div>
Default	Disabled.
Options	<i>class-name</i> —Name of the forwarding class. The forwarding class can be one of the predefined forwarding classes (best-effort, assured-forwarding, expedited-forwarding, network-control) or it can be a user-defined forwarding class.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Prioritizing Snooped and Inspected Packet on page 423 • Understanding Junos OS CoS Components for EX Series Switches • Understanding DHCP Snooping (non-ELS) on page 393 • Understanding ARP Spoofing and Inspection on page 449

forwarding-options

```
Syntax forwarding-options {
    dhcp-security {
        arp-inspection;
        group group-name {
            interface interface-name {
                static-ip ip-address {
                    mac mac-address;
                }
            }
            overrides {
                no-option82;
                (trusted | untrusted);
            }
        }
        ip-source-guard;
        no-dhcp-snooping;
        option-82 {
            circuit-id {
                prefix {
                    host-name;
                    logical-system-name;
                    routing-instance-name;
                }
                use-interface-description (device | logical);
                use-vlan-id;
            }
            remote-id {
                host-name hostname;
                use-interface-description (device | logical);
                use-string string;
            }
            vendor-id {
                use-string string;
            }
        }
    }
    filter (VLANs) {
        input filter-name;
        output filter-name;
    }
    flood {
        input filter-name;
    }
}
```

Chassis: EX4600 and
QFX Series

```
forwarding options profile-name {
    num-65-127-prefix number;
}
```


Chassis: EX4600 and QFX Series	<pre>forwarding-options lpm-profile { prefix-65-127-disable; unicast-in-lpm; }</pre>
Chassis: EX4600 and QFX Series	<pre>forwarding-options custom-profile { l2-entries l3-entries lpm-entries { num-banks <i>number</i>; } }</pre>
Hierarchy Level	<pre>[edit], [edit bridge-domains <i>bridge-domain-name</i>], [edit vlans <i>vlan-name</i>]</pre> <pre>[edit chassis (QFX Series)]</pre>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 11.3 for QFX Series switches.</p> <p>Hierarchy level [edit vlans <i>vlan-name</i>] introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Hierarchy level [edit bridge-domains <i>bridge-domain-name</i>] introduced in Junos OS Release 14.1 for MX Series routers.</p> <p>custom-profile option introduced in Junos OS Release 15.1x53-D30 for QFX5200 Series switches only.</p>

Description Configure a unified forwarding table profile to allocate the amount of memory available for the following:

- MAC addresses.
- Layer 3 host entries.
- Longest prefix match table entries.

This feature enables you to select a profile that optimizes the amount of memory available for various types of forwarding-table entries based on the needs of your network. For example, for a switch that handles a great deal of Layer 2 traffic, such as a virtualized network with many servers and virtualized machines, you would choose the **l2-profile-one**, which allocates the highest amount of memory to MAC addresses.

You configure the memory allocation for LPM table entries differently, depending on whether you are using Junos OS Release 13.2X51-D10 or Junos OS Release 13.2X51-D15 and later. For more information about configuring memory allocation for LPM table entries, see *Configuring the Unified Forwarding Table on Switches*.

The **num-65-127-prefix *number*** statement is not supported on the **custom-profile** and the **lpm-profile**. The **prefix-65-127-disable** and **unicast-in-lpm** statements are supported only on the **lpm-profile**.

When you commit a configuration with a forwarding table profile change, in most cases the Packet Forwarding Engine restarts automatically to apply the new parameters, which brings the data interfaces down and then up again.

However, starting with Junos OS Releases 14.1X53-D40, 15.1R5, and 16.1R3, for a Virtual Chassis or Virtual Chassis Fabric (VCF) comprised of EX4600 or QFX5100 switches, the Packet Forwarding Engine in member switches does not automatically restart upon configuring and committing a unified forwarding table profile change. This behavior avoids having Virtual Chassis or VCF instability and a prolonged convergence period if a profile change is propagated to member switches and multiple Packet Forwarding Engines all restart at the same time. In this environment, instead of automatically restarting when you initially commit a profile configuration change, the message **Reboot required for configuration to take effect** is displayed at the master switch CLI prompt, notifying you that the profile change does not take effect until the next time you restart the Virtual Chassis or VCF. The profile configuration change is propagated to member switches that support this feature, and a reminder that a reboot is required to apply this pending configuration change appears in the system log of the master switch and applicable member switches. You then enable the profile change subsequently during a planned downtime period using the **request system reboot** command, which quickly establishes a stable Virtual Chassis or VCF with the new configuration.



NOTE: You should plan to make unified forwarding table profile changes only when you are ready to perform a Virtual Chassis or VCF system reboot *immediately* after committing the configuration update. Otherwise, in the intervening period between committing the configuration change and rebooting the Virtual Chassis or VCF, the system can become inconsistent if

a member experiences a problem and restarts. In that case, the new configuration takes effect on the member that was restarted, while the change is not yet activated on all the other members.

.....
The remaining statements are explained separately. See [CLI Explorer](#).

Options **profile-name**—name of the profile to use for memory allocation in the unified forwarding table. [Table 35 on page 792](#) lists the profiles you can choose that have set values and the associated values for each type of entry.

On QFX5200 Series switches only, you can also select **custom-profile**. This profile enables you to allocate from one to four banks of shared hash memory to a specific type of forwarding-table entry. Each shared hash memory bank can store a maximum of the equivalent of 32,000 IPv4 unicast addresses.

Table 35: Unified Forwarding Table Profiles

Profile Name	MAC Table	Host Table (unicast and multicast addresses)					
	MAC Addresses	IPv4 unicast	IPv6 unicast	IPv4 (*, G)	IPv4 (S, G)	IPv6 (*, G)	IPv6 (S, G)
l2-profile-one	288K	16K	8K	8K	8K	4K	4K
l2-profile-two	224K	80K	40K	40K	40K	20K	20K
l2-profile-three (default)	160K	144K	72K	72K	72K	36K	36K
l3-profile	96K	208K	104K	104K	104K	52K	52K
lpm-profile*	32K	16K	8K	8K	8K	4K	4K

* This profile supports only IPv4 in Junos OS Release 13.2X51-D10. Starting in Junos OS Release 13.2X51-D15, the **lpm-profile** supports IPv4 and IPv6 entries.



NOTE: If the host stores the maximum number of entries for any given type, the entire table is full and is unable to accommodate *any* entries of any other type. For information about valid combinations of table entries see *Understanding the Unified Forwarding Table*.

l2-entries | l3-entries | lpm-entries—(custom-profile only) Select a type of forwarding-table entry—Layer 2, Layer 3, or LPM—to allocate a specific number of shared memory banks. You configure the amount of memory to allocate for each type of entry separately.

num-banks *number*—(custom-profile only) Specify the number of shared memory banks to allocate for a specific type of forwarding-table entry. Each shared memory bank stores the equivalent of 32,000 IPv4 unicast addresses.

Range: 0 through 4.



NOTE: There are four shared memory banks, which can be allocated flexibly among the three types of forwarding-table entries. To allocate

no shared memory for a particular entry type, specify the number 0. When you commit the configuration, the system issues a commit check to ensure that you have not configured more than four memory banks. You do not have to configure all four shared memory banks. By default, each entry type is allocated the equivalent of 32,000 IPv4 unicast addresses in shared memory.


Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• <i>Understanding the Unified Forwarding Table</i>• <i>Example: Configuring a Unified Forwarding Table Custom Profile</i>• <i>Configuring Traffic Forwarding and Monitoring</i>
------------------------------	--

fpc (DDoS)

Syntax	<pre>fpc slot-number; bandwidth-scale percentage; burst-scale percentage; disable-fpc; }</pre>
Hierarchy Level	<ul style="list-style-type: none">For MX Series routers, T4000 routers, and EX9200 switches: <pre>[edit system ddos-protection protocols protocol-group (aggregate packet-type)]</pre>For PTX Series routers and QFX Series switches: <pre>[edit system ddos-protection protocols protocol-group (aggregate packet-type)]</pre>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.</p> <p>Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.</p>
Description	(MX Series routers with only MPCs, T4000 routers with only FPC5s, PTX Series routers, EX9200 switches, or QFX Series switches) Modify the aggregate or packet-type policer on the specified line card.
Options	<p>slot-number—Slot number of the card.</p> <p>Range: Depends on the router or switch model</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537

global (DDoS)

Syntax	<pre> global { disable-fpc; disable-logging; disable-routing-engine; flow-detection; flow-level-control; flow-detection-mode; flow-report-rate; violation-report-rate; } </pre>
Hierarchy Level	[edit system ddos-protection]
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p> <p>Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.</p>
Description	<p>(MX Series routers with only MPCs, T4000 routers with only FPC5s, PTX Series routers, EX9200 switches, or QFX Series switches) Modify DDoS policers, event logging, and flow detection globally for all protocols.</p>
<div>  <p>NOTE: The following statements are not supported on PTX Series routers and QFX Series switches: disable-routing-engine, flow-detection, flow-report-rate, and violation-report-rate.</p> </div>	
<p>The remaining statements are explained separately. See CLI Explorer.</p>	
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Disabling DDoS Protection Policers and Logging Globally on page 536

group (DHCP Security)

Syntax

```
group group-name {
  interface interface-name {
    static-ip ip-address {
      mac mac-address;
    }
    static-ipv6 ip-address {
      mac mac-address;
    }
  }
  overrides {
    no-dhcpv6-options;
    no-option16;
    no-option18;
    no-option37;
    no-option82;
    trusted;
    untrusted;
  }
}
```

Hierarchy Level [edit vlans *vlan-name* forwarding-options **dhcp-security**]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX series.
Support for the **static-ipv6** and **no-option37** statements introduced in Junos OS Release 13.2X51-D20 for EX Series switches.

Description Specify the name of a group of access interfaces that you want to configure for DHCP security attributes that are different from the attributes set for other interfaces in the VLAN. A group must contain at least one 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 Static DHCP IP Addresses for DHCP snooping \(ELS\) on page 404](#)
- [Enabling a Trusted DHCP Server \(ELS\) on page 372](#)
- [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

group (DHCP Security for MX Series)

Syntax	<pre> group <i>group-name</i> { interface <i>interface-name</i> { static-ip <i>ip-address</i> { mac <i>mac-address</i>; } } overrides { no-option82; trusted; untrusted; } } </pre>
Hierarchy Level	[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]
Release Information	<p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Support for the static-ipv6 and no-option37 statements introduced in Junos OS Release 13.2X51-D20 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1 for the MX Series.</p>
Description	<p>Specify the name of a group of access interfaces that you want to configure for DHCP security attributes that are different from the attributes set for other interfaces in the VLAN or bridge domain. A group must contain at least one interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static DHCP IP Addresses for DHCP snooping (MX routers) on page 406 • Enabling a Trusted DHCP Server (MX Series Routers) on page 373 • Understanding DHCP Snooping (non-ELS) on page 393

group-type (Unknown Unicast Forwarding)

Syntax	group-type (<i>none</i> layer-2)
Hierarchy Level	[edit forwarding-options next-hop-group]
Release Information	Statement introduced in Junos OS Release 14.2 for EX Series switches.
Description	Configure the type of addresses to be used in the next-hop group.
Options	<i>none</i> —Next-hop group uses Layer 2 addresses. <i>layer-2</i> —Specify a next-hop group that uses Layer 2 addresses.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Unknown Unicast Forwarding (ELS) on page 614• Configuring Mirroring on EX9200 Switches to Analyze Traffic (CLI Procedure)

host-name

Syntax	<code>host-name <i>host-name</i>;</code>
Hierarchy Level (EX Series)	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 remote-id]</code>
Hierarchy Level (MX Series)	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security remote-id option-82]</code>
Release Information	Statement introduced in Junos OS Release 13.2X50-D10. Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	Use the hostname of the switching device as the remote-id suboption of DHCP option 82 (also known as the DHCP relay agent information option) in DHCP request packet headers before forwarding or relaying requests to a DHCP server. This suboption provides a trusted identifier for the host system that has forwarded or relayed requests to the server.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Setting Up DHCP Option 82 on the Switch with No Relay (ELS) on page 439 • Configuring DHCP Option 82 on a Router with Bridge Domain on page 437 • RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046

host-vpn

```
Syntax host-vpn {
    connections {
        connection-name {
            children {
                child-name {
                    esp-proposal esp-proposal;
                    local-traffic-selector {
                        (ipv4-prefix ipv4-prefix | ipv6-prefix ipv6-prefix);
                        port port;
                        protocol protocol;
                    }
                    mode (transport | tunnel);
                    rekey-time rekey-time;
                    remote-traffic-selector {
                        (ipv4-prefix ipv4-prefix | ipv6-prefix ipv6-prefix);
                        port port;
                        protocol protocol;
                    }
                }
            }
        }
        dpd-delay dpd-delay;
        ike-proposal ike-proposal;
        local {
            id local-id;
        }
        local-address {
            (ipv4 ipv4-address | ipv6 ipv6-address);
        }
        rekey-time rekey-time;
        remote {
            id remote-id;
        }
        remote {
            id remote-id;
        }
        remote-address {
            (ipv4 ipv4-address | ipv6 ipv6-address);
        }
    }
    ike-log {
        filename filename;
        level level;
    }
    ike-secrets {
        ike-secret {
            id id;
            secret (ascii-text ascii-text | hexadecimal hexadecimal);
        }
    }
}
```

Hierarchy Level	[edit security]
Release Information	Statement introduced in Junos OS Release 18.3R1 Evolved.
Description	Configure a host-to-host VPN type of IPsec connection. The remaining statements are explained separately.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • show security host-vpn security-associations on page 1236 • clear security host-vpn security-associations on page 1070 • show security host-vpn version on page 1239

id

Syntax	<pre>id { mac-address mac-address; port-id port-id-number; }</pre>
Hierarchy Level	[edit security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	Specify a MAC address and a port that traffic on the link must be from to be accepted by the interface when MACsec is enabled using static secure association key (SAK) security mode.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

id (MACsec for MX Series)

Syntax	<pre>id { mac-address <i>mac-address</i>; port-id <i>port-id-number</i>; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	Specify a MAC address and a port that traffic on the link must be from to be accepted by the interface when MACsec is enabled using static secure association key (SAK) security mode.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

identity

Syntax	<pre>identity <i>identity-name</i>;</pre>
Hierarchy Level	[edit security ike]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the identity of the remote certificate name if the identity cannot be learned through IKE (ID payload or IP address).
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an IKE Policy for Digital Certificates for an ES PIC on page 182

ike (Security)

```
Syntax  ike {
        policy ike-peer-address {
            description policy-description;
            encoding (binary | pem);
            identity identity-name;
            local-certificate certificate-filename;
            local-key-pair private-public-key-file;
            mode (aggressive | main);
            pre-shared-key (ascii-text key | hexadecimal key);
            proposals [ proposal-names ];
        }
        proposal ike-proposal-name {
            authentication-algorithm (md5 | sha1);
            authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
            dh-group (group1 | group2);
            encryption-algorithm (3des-cbc | des-cbc);
            lifetime-seconds seconds;
        }
    }
```

Hierarchy Level [edit security]

Release Information Statement introduced before Junos OS Release 7.4.

Description (Encryption interface on M Series and T Series routers only) Configure IKE.

Options The remaining statements are explained separately.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring an IKE Proposal for Dynamic SAs](#)
- [Configuring an IKE Policy for Preshared Keys on page 44](#)

ike-log

Syntax	<pre>ike-log { filename <i>filename</i>; level <i>level</i>; }</pre>
Hierarchy Level	[edit security host-vpn]
Release Information	Statement introduced in Junos OS Evolved Release 18.3R1.
Description	Configure IKE logging details.
Options	<p>filename <i>filename</i>—Specify the filename for logging—for example, <code>/var/log/<i>filename</i>.log</code>. Default: <code>/var/log/charon.log</code></p> <p>level <i>level</i>—Specify the logging level (how much detail is included) of the IKE daemon's log messages. Following are the levels of logging available:</p> <ul style="list-style-type: none">• 0: Very basic auditing logs (for example SA up/SA down).• 1: Generic control flow with errors. This is the default.• 2: More detailed debugging control flow.• 3: Including RAW (unprocessed) data dumps in hex. <p>Range: 0 (minimal logging) through 3 Default: 1</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

ike-secrets

Syntax

```
ike-secrets {
  ike-secret {
    id id;
    secret (ascii-text ascii-text | hexadecimal hexadecimal);
  }
}
```

Hierarchy Level [edit security host-vpn]

Release Information Statement introduced in Junos OS Evolved Release 18.3R1.

Description Configure IKE shared secret details. If the shared secret passed between devices does not match, a session is not set up.



NOTE: To configure a host-to-host VPN connection, you must configure the `ike-secrets` statement.

Options *ike-secret*—Specify the name of the IKE secret.

id id—Specify the identity that the secret belongs to—for example, an IP address, a domain name, or an e-mail address. This identity matches local and remote identities as exchanged in the IKE security association (SA) negotiation at the **[edit security host-vpn connections]** hierarchy level.

*secret (ascii-text *ascii-text* | hexadecimal *hexadecimal*)*—Define the preshared private key associated with the identity in either ASCII or hexadecimal format.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- [connections \(Host VPN\) on page 708](#)

include-sci

Syntax	<code>include-sci;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.</p> <p>Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.</p>
Description	<p>Specifies that the SCI tag should be appended to each packet on a link that has enabled MACsec.</p> <p>You must enable SCI tagging on a switch that is enabling MACsec on an Ethernet link connecting to an EX4300 switch.</p> <p>SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. This option is, therefore, not available on EX4300 switches.</p> <p>You should only use this option when connecting a switch to an EX4300 switch, or to a host device that requires SCI tagging. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.</p>
Default	<p>SCI tagging is enabled on EX4300 switches that have enabled MACsec using static connectivity association key (CAK) security mode, by default.</p> <p>SCI tagging is disabled on all other interfaces, by default.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228

include-sci (MACsec for MX Series)

Syntax	include-sci;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specifies that the SCI tag should be appended to each packet on a link that has enabled MACsec.</p> <p>This option is used only when connecting a router to a host device that requires SCI tagging. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.</p>
Default	SCI tagging is not enabled by default.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

interface (Access Port Security)

Syntax

```
interface (all | interface-name) {
  allowed-mac {
    mac-address-list;
  }
  (dhcp-trusted | no-dhcp-trusted);
  fcoe-trusted;
  mac-limit limit action (drop | log | none | shutdown);
  no-allowed-mac-log;
  persistent-learning;
  static-ip ip-address {
    vlan vlan-name;
    mac mac-address;
  }
  static-ipv6 ip-address {
    vlan vlan-name;
    mac mac-address;
  }
}
vlan vlan-name {
  mac-limit limit action (drop | log | none | shutdown);
}
```

Hierarchy Level [edit [ethernet-switching-options secure-access-port](#)]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the **ipv6-source-guard** statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Apply port security features to all interfaces or to the specified interface.

Options

all—Apply port security features to all interfaces.

interface-name—Apply port security features to the specified interface.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation


- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Example: Protecting Against DHCP Snooping Database Attacks on page 415](#)
- [Example: Protecting against Ethernet Switching Table Overflow Attacks on page 354](#)
- [Example: Protecting against DHCP Starvation Attacks on page 347](#)

- [Example: Protecting against Rogue DHCP Server Attacks on page 351](#)
- [Configuring MAC Limiting \(non-ELS\) on page 341](#)
- [Enabling a Trusted DHCP Server \(non-ELS\) on page 373](#)
- [Configuring Static DHCP IP Addresses for DHCP snooping \(non-ELS\) on page 405](#)

interface (DHCP Security for MX Series)

Syntax	<pre>interface <i>interface-name</i> { static-ip <i>ip-address</i> { mac <i>mac-address</i>; } }</pre>
Hierarchy Level	[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security group <i>group-name</i>]
Release Information	Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	<p>Configure an interface for a static IP address to MAC address binding (IP-MAC binding) or configure an interface to belong to a group within the bridge domain that has DHCP security attributes that are different from the attributes of other interfaces in the bridge domain.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static DHCP IP Addresses for DHCP snooping (MX routers) on page 406

interface (RA Guard)

Syntax	<pre>interface <i>interface-name</i> { mark-interface (trusted block); policy <i>policy-name</i> (stateful stateless); }</pre>
Hierarchy Level	[edit forwarding-options access-security router-advertisement-guard]
Release Information	Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Statement introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Configure IPv6 Router Advertisement (RA) guard on an interface. In an IPv6 deployment, RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in a policy.</p> <p>Before you can configure RA guard on an interface, you must first configure a policy at the [edit forwarding-options access-security router-advertisement-guard] hierarchy level. The policy is then applied to an interface at the [edit forwarding-options access-security router-advertisement-guard interface <i>interface-name</i>] hierarchy level.</p>
	<p> NOTE: If you apply an RA guard policy on an interface, you must enable RA guard on the VLAN that is associated with that interface by using the <code>vlan</code> statement at the [edit forwarding-options access-security router-advertisement-guard] hierarchy level.</p>
	<p>The remaining statements are explained separately. See CLI Explorer.</p>
Options	<i>interface-name</i> —Configure RA guard parameters on the specified interface.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514

interface (Secure Access Port)

Syntax	<pre> interface (all <i>interface-name</i>) { allowed-mac <i>mac-address-list</i>; (dhcp-trusted no-dhcp-trusted); mac-limit <i>limit</i> action <i>action</i>; no-allowed-mac-log; static-ip <i>ip-address</i> { vlan <i>vlan-name</i>; mac <i>mac-address</i>; } } </pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	<p>Apply port security features to all interfaces or to the specified interface.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Options	<p>all—Apply port security features to all interfaces. Does not apply to QFabric systems.</p> <p><i>interface-name</i>—Apply port security features to the specified interface.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding How to Protect Access Ports from Common Attacks on page 6 • Understanding MAC Limiting and MAC Move Limiting for Port Security • Understanding and Using Trusted DHCP Servers on page 371 • Configuring MAC Limiting (QFX Switches) on page 344

interface (Static MAC Bypass)

Syntax	<code>interface [<i>interface-names</i>];</code>
Hierarchy Level	[edit protocols authentication-access-control]
Release Information	Statement introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.
Description	Configure interfaces on which the specified MAC addresses are allowed to bypass RADIUS authentication and allowed to connect to the LAN without authentication.
Options	<i>interface-names</i> —List of interfaces.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	

interface (Storm Control)

Syntax	<pre>interface (all <i>interface-name</i>) { bandwidth <i>bandwidth</i>; level <i>level</i>; multicast; no-broadcast; no-multicast; no-registered-multicast; no-unknown-unicast; no-unregistered-multicast; }</pre>
Hierarchy Level	[edit ethernet-switching-options storm-control]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure storm control on all interfaces or on the specified interface.
Default	<ul style="list-style-type: none"> On EX2200, EX3200, EX3300, EX4200, and EX6200 switches—Storm control does not apply by default to multicast traffic. The factory default configuration enables storm control for broadcast and unknown unicast traffic on all switch interfaces, with the storm control level set to 80 percent of the combined broadcast and unknown unicast streams. On EX4500 and EX8200 switches—Storm control applies to broadcast, multicast, and unknown unicast traffic. The factory default configuration enables storm control on all switch interfaces, with the storm control level set to 80 percent of the combined broadcast, multicast, and unknown unicast streams.
Options	<p>all—All interfaces. The storm control settings configured with the all option affect only those interfaces that have not been individually configured for storm control.</p> <p><i>interface-name</i>—Name of an interface. The storm control settings configured with the <i>interface-name</i> option override any settings configured with the all option.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Autorecovery for Port Security Events on page 635 Enabling and Disabling Storm Control (non-ELS) on page 626

interface (Unknown Unicast Forwarding)

Syntax	<code>interface <i>interface-name</i>;</code>
Hierarchy Level	<ul style="list-style-type: none">For platforms with ELS: <code>[edit switch-options unknown-unicast-forwarding vlan <i>vlan-name</i>]</code>For platforms without ELS: <code>[edit ethernet-switching-options unknown-unicast-forwarding vlan <i>vlan-name</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Hierarchy level <code>[edit switch-options]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p>
Description	Specify the interface to which unknown unicast packets will be forwarded.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"><code>show vlans</code>show ethernet-switching table on page 1198Understanding and Preventing Unknown Unicast Forwarding on page 613

interface-mac-limit

Syntax

```
interface-mac-limit {
    limit
    disable;
    packet-action ;
}
```

Hierarchy Level

```
[edit bridge-domains bridge-domain-name bridge-options],
[edit bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit logical-systems logical-system-name bridge-domains bridge-domain-name
bridge-options],
[edit logical-systems logical-system-name bridge-domains bridge-domain-name
bridge-options interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name
bridge-domains bridge-domain-name bridge-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name
bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name
switch-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name
switch-options interface interface-name],
[edit logical-systems logical-system-name switch-options],
[edit logical-systems logical-system-name switch-options interface interface-name],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name
bridge-options],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name
bridge-options interface interface-name],
[edit routing-instances routing-instance-name switch-options],
[edit routing-instances routing-instance-name switch-options interface interface-name],
[edit switch-options],
[edit switch-options],
[edit switch-options interface interface-name],
[edit switch-options interface interface-name],
[edit vlans vlan-name switch-options],
[edit vlans vlan-name switch-options interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 8.4.

Support for the **switch-options** statement added in Junos OS Release 9.2.

Support for top-level configuration for the **virtual-switch** type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy supported this statement only for a VPLS instance or a bridge domain configured within a virtual switch.

Support for logical systems added in Junos OS Release 9.6.

[edit switch-options], [edit switch-options interface *interface-name*], [edit vlans *vlan-name* switch-options], and [edit vlans *vlan-name* switch-options interface *interface-name*] hierarchy levels introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure a limit to the number of MAC addresses that can be learned from a bridge domain, VLAN, virtual switch, or set of bridge domains or VLANs.



NOTE: For multichassis link aggregation (MC-LAG) peers in active-active mode, configuring the `interface-mac-limit` statement or changing the `interface-mac-limit` configuration when traffic is flowing can cause the MAC entries to be out of synchronization between the two MC-LAG peers, which might result in flooding. To avoid flooding, you must either halt traffic forwarding and then configure the `interface-mac-limit` statement or use the `commit at` configuration statement to commit the changes at the same time in both the peer nodes.

Alternatively, if flooding does occur, you can clear the bridge MAC table on both the routers or switches by using the `clear bridge mac-table` command. Running this command ensures that the MAC entries are re-learned and in synchronization between both the peers.

Default The default MAC limit varies with the platform.

Options **disable**—Disables the global `interface-mac-limit` configuration on an interface and sets the maximum `interface-mac-limit` that is permitted on the device.

limit—Sets the maximum number of MAC addresses learned from an interface.

Range: 1 through <default MAC limit> MAC addresses per interface. Range is platform specific.

If you configure both **disable** and **limit**, **disable** takes precedence and `packet-action` is set to **none**. The remaining statement is explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Understanding Layer 2 Learning and Forwarding for Bridge Domains*
- *Layer 2 Learning and Forwarding for VLANs Overview*
- *Understanding Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports*
- *Layer 2 Learning and Forwarding for VLANs Acting as a Switch for a Layer 2 Trunk Port*


interface-shutdown-action

Syntax	<code>interface-shutdown-action [soft-shutdown hard-shutdown]</code>
Hierarchy Level	<code>[edit switch-options]</code>
Release Information	Statement introduced in Junos OS Release 14.1X53-D40 for EX Series switches
Description	<p>Configure storm control to shut down interfaces or temporarily disable interfaces. This action can be done in addition to the default switching device action for storm control (dropping packets).</p> <p>Storm control enables the switching device to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the storm control level or storm control bandwidth—is exceeded, thus preventing packets from proliferating and degrading the LAN.</p> <p>When you include the interface-shutdown-action statement at the <code>[edit switch-options]</code> hierarchy level, the behavior is to temporarily disable interfaces when the storm control level threshold is exceeded.</p> <p>When the configuration statement recovery-timeout is included under the <code>[edit interfaces ether-options ethernet-switch-profile]</code> hierarchy level, a temporarily disabled port will come up again after the specified time interval.</p>
Default	Default behavior for this configuration is soft shutdown.
Options	<ul style="list-style-type: none"> • hard-shutdown—When the storm control level threshold is exceeded, the physical interface is brought down. • soft-shutdown—When the storm control level threshold is exceeded, data traffic is blocked and only control traffic is allowed to pass.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches</i> • Understanding Storm Control on page 622

interfaces (MACsec)

Syntax	<pre>interfaces <i>interface-name</i> { <i>connectivity-association</i> <i>connectivity-association-name</i>; }</pre>
Hierarchy Level	[edit security <i>macsec</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
Description	<p>Applies the specified connectivity association to the specified interface to enable MACsec.</p> <p>One connectivity association can be applied to multiple interfaces.</p> <p>You must always use this statement to apply a connectivity association to an interface to enable MACsec. You must complete this configuration step regardless of whether MACsec is enabled using static connectivity association key (CAK) security mode or static secure association key (SAK) security mode.</p> <p>If you are enabling MACsec using static SAK security mode and need to configure MACsec on inbound and outbound traffic on the same interface, you must configure a connectivity association with one secure channel for inbound traffic and a second secure channel for outbound traffic. The connectivity association is then applied to the interface using this statement to enable MACsec for traffic entering and leaving the interface.</p>
Default	Interfaces are not associated with any connectivity associations, by default.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228

interfaces (MACsec for MX Series)

Syntax	<pre> interfaces <i>interface-name</i> { connectivity-association <i>connectivity-association-name</i>; } </pre>
Hierarchy Level	[edit security macsec]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Applies the specified connectivity association to the specified interface to enable MACsec.</p> <p>One connectivity association can be applied to multiple interfaces.</p> <p>You must always use this statement to apply a connectivity association to an interface to enable MACsec. You must complete this configuration step regardless of whether MACsec is enabled using static connectivity association key (CAK) security mode or static secure association key (SAK) security mode.</p> <p>If you are enabling MACsec using static SAK security mode and need to configure MACsec on inbound and outbound traffic on the same interface, you must configure a connectivity association with one secure channel for inbound traffic and a second secure channel for outbound traffic. The connectivity association is then applied to the interface using this statement to enable MACsec for traffic entering and leaving the interface.</p> <div>  <p>NOTE: Starting in Junos OS Release 16.1R2, when Media Access Control Security (MACsec) is enabled on an interface, the interface flow control capability is enabled by default, regardless of the configuration that you set using the (flow-control no-flow-control) statement at the [edit interfaces <i>interface-name</i> gige-ether-options] hierarchy level. When MACsec is disabled, interface flow control is restored to the configuration that you set using the flow-control statement at the [edit interfaces] hierarchy level. When MACsec is enabled, additional header bytes are added to the packet by the MACsec PHY. With line rate traffic, when MACsec is enabled and flow control is disabled, the pause frames sent by the MACsec PHY are terminated by the MIC's MAC (enhanced 20-port Gigabit Ethernet MICs on MX Series routers) and not transferred to the Packet Forwarding Engine, causing framing errors. Therefore, when MACsec is enabled on an interface, flow control is also automatically enabled on such an interface.</p> </div>
Default	Interfaces are not associated with any connectivity associations, by default.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Media Access Control Security \(MACsec\) on MX Series Routers on page 268](#)

internal

Syntax

```
internal {
  security-association {
    manual {
      direction (bidirectional | inbound | outbound) {
        protocol esp;
        spi spi-value;
        encryption {
          algorithm 3des-cbc;
          key ascii-text ascii-text-string;
        }
      }
    }
  }
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

Description (Junos-FIPS only) Define an internal security association (SA) for internal Routing-Engine-to-Routing-Engine communication.

Options The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- [Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 211](#)
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

ipsec (Security)

```
Syntax ipsec {
    security-association {
        manual {
            direction (bidirectional | inbound | outbound) {
                protocol esp;
                spi spi-value;
                encryption {
                    algorithm 3des-cbc;
                    key (ascii-text ascii-text-string | hexadecimal hexadecimal-string);
                }
            }
        }
    }
    policy ipsec-policy-name {
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposals [ proposal-names ];
    }
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-sha1-96 | hmac-sha2-256);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol (ah | esp | bundle);
    }
    security-association name {
        dynamic {
            ipsec-policy policy-name;
            replay-window-size (32 | 64);
        }
        manual {
            direction (inbound | outbound | bi-directional) {
                authentication {
                    algorithm (hmac-sha1-96 | hmac-sha2-256);
                    key (ascii-text key | hexadecimal key);
                }
                auxiliary-spi auxiliary-spi-value;
                encryption {
                    algorithm (des-cbc | 3des-cbc);
                    key (ascii-text key | hexadecimal key);
                }
                protocol (ah | esp | bundle);
                spi spi-value;
            }
        }
        mode (tunnel | transport);
    }
    traceoptions {
        file <files number> < size size>;
        flag all;
        flag database;
    }
}
```

```
flag general;  
flag ike;  
flag parse;  
flag policy-manager;  
flag routing-socket;  
flag timer;  
}  
}
```

Hierarchy Level [edit security]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure IPsec on encryption interfaces.



NOTE: You must configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Options The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Security Associations for IPsec on an ES PIC on page 37](#)

ip-source-guard

Syntax	<code>ip-source-guard;</code>
Hierarchy Level	<ul style="list-style-type: none"> For platforms with ELS: <div>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</div> For platforms without ELS: <div>[edit ethernet-switching-options secure-access-port <i>vlan</i> (all <i>vlan-name</i>)]</div>
Release Information	<p>Statement introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 17.3 for QFX Series switches.</p>
Description	<p>Perform IP source guard checking on packets sent from access interfaces. Validate source IP addresses and source MAC addresses on all VLANs or on the specified VLAN or VLAN range. Forward packets with valid addresses and drop those with invalid addresses.</p> <ul style="list-style-type: none"> ip-source-guard—Enable IP source guard checking. no-ip-source-guard—(Not available in [edit vlans <i>vlan-name</i> forwarding-options dhcp-security]) Disable IP source guard checking. <p>If you configure IP source guard at the [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] hierarchy level:</p> <ul style="list-style-type: none"> IP source guard can be configured only for a specific VLAN, not for a list or a range of VLAN IDs. DHCP snooping is automatically enabled. <p>See “Configuring IP Source Guard (ELS)” on page 465 for more information about this configuration.</p> <p>If you configure IP source guard at the [edit ethernet-switching-options secure-access-port <i>vlan</i> (all <i>vlan-name</i>)] hierarchy level:</p> <ul style="list-style-type: none"> You must enable DHCP snooping on all VLANs if you configure IP source guard on all VLANs. You must enable DHCP snooping for the specific VLAN if you configure IP source guard on that specific VLAN. Otherwise, the default behavior of no DHCP snooping applies to that VLAN. <p>See “Enabling DHCP Snooping (non-ELS)” on page 400 for more information about this configuration.</p>



NOTE: On EX9200 switches, IP source guard is not supported in an MC-LAG scenario.

Default	Disabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 467• Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 476• Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487• Configuring IP Source Guard (non-ELS) on page 461• Configuring IP Source Guard (ELS) on page 465


ip-source-guard (MX Series)

Syntax	<code>ip-source-guard;</code>
Hierarchy Level	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code>
Release Information	Hierarchy level <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.
Description	<p>Perform IP source guard checking on packets sent from access interfaces. Validate source IP addresses and source MAC addresses on all bridge domains or on the specified bridge domain or bridge domain range. Forward packets with valid addresses and drop those with invalid addresses.</p> <ul style="list-style-type: none"> <code>ip-source-guard</code>—Enable IP source guard checking. <p>If you configure IP source guard at the <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> hierarchy level:</p> <ul style="list-style-type: none"> IP source guard can be configured only for a specific bridge domain, not for a list or range of bridge domains. DHCP snooping is automatically enabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring IP Source Guard to Mitigate the Effects of Source IP Address Spoofing and Source MAC Address Spoofing on page 497 Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 497


source-ip-address-list

Syntax	<code>source-ip-address-list <i>address-list-name</i>;</code>
Hierarchy Level	<p>[edit forwarding-options access-security router-advertisement-guard policy <i>policy-name</i> discard]</p> <p>[edit forwarding-options access-security router-advertisement-guard policy <i>policy-name</i> accept match-list]</p>
Release Information	<p>Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.</p> <p>Statement introduced in Junos OS Release 16.1 for EX Series switches.</p>
Description	<p>Configure a list of IPv6 addresses for an IPv6 Router Advertisement (RA) guard policy to validate the source IPv6 address of an incoming RA message against the IPv6 addresses in this list. RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in the policy.</p> <p>You can use a list of IPv6 addresses for validating RA messages as part of either an accept policy or a discard policy. Before you can include a list in an RA policy, you must configure the list name at the [edit policy-options prefix-list] hierarchy level. When RA guard is enabled by using an accept policy, any RA messages that match the conditions defined in the policy are forwarded, and RA messages that do not match the conditions are dropped. When RA guard is enabled by using a discard policy, any RA messages that match the conditions are dropped, and RA messages that do not match the conditions are forwarded.</p>
Options	<i>address-list-name</i> —Configure a list of IPv6 addresses to use in an RA guard policy. The policy is used to validate the source of an incoming RA message by comparing the IPv6 address of the RA message to the IPv6 addresses contained in the list.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514

ipv6-source-guard

Syntax	<code>ipv6-source-guard;</code>
Hierarchy Level	<ul style="list-style-type: none"> For platforms with Enhanced Layer 2 Software (ELS): <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security];</code> For platforms without ELS: <code>[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>)]</code>
Release Information	<p>Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches.</p> <p>Support at the <code>[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>)]</code> hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 17.3R1 for QFX Series switches.</p>
Description	<p>Perform IPv6 source guard checking on packets sent from access interfaces. Validate source IP addresses and source MAC addresses on all VLANs or on the specified VLAN. Forward packets with valid addresses and drop those with invalid addresses.</p>
	<p> NOTE: If you configure the <code>ipv6-source-guard</code> statement at the <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> hierarchy level, DHCPv6 snooping is automatically enabled for the specified VLAN.</p> <p>If you configure the <code>ipv6-source-guard</code> statement at the <code>[edit ethernet-switching-options secure-access-port vlan <i>vlan-name</i>]</code> hierarchy level, you must also enable DHCPv6 snooping for the specified VLAN.</p>
Default	Disabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 492 Configuring IP Source Guard (ELS) on page 465

ipv6-source-guard-sessions

Syntax	<pre> ipv6-source-guard-sessions { max-number <i>max-number</i>; } </pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Specify the maximum number of IPv6 source guard sessions for TCAM space provisioning.
	<p> NOTE: After setting or changing the maximum number of IPv6 source guard sessions and committing the configuration, you must reboot the switch for the configuration to take effect.</p>
Default	Disabled.
Options	max-number <i>max-number</i> —The maximum number of IPv6 source guard sessions. Range: 50 through 300.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 492 • Configuring IP Source Guard (ELS) on page 465

key (Authentication Keychain)

Syntax	<pre>key key { algorithm (md5 hmac-sha-1); options (basic isis-enhanced); key-name authentication-key-name; secret secret-data; start-time yyyy-mm-dd.hh:mm:ss; }</pre>
Hierarchy Level	[edit security authentication-key-chains key-chain <i>key-chain-name</i>]
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Statement introduced in Junos OS Release 17.4.</p>
Description	Configure the authentication element.
Options	<p>key—Each key within a keychain is identified by a unique integer value.</p> <p>Range: 0 through 63</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols</i> • <i>Example: Configuring BFD Authentication for Securing Static Routes</i> • <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

key (Junos FIPS)

Syntax	<code>key (ascii-text <i>key</i> hexadecimal <i>key</i>);</code>
Hierarchy Level	[edit security ipsec internal security-association manual direction encryption]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	The key used for the internal Routing-Engine-to-Routing-Engine IPsec security association (SA) configuration.
Options	<i>ascii-text-key</i> —The encrypted ASCII text key. <i>hexadecimal key</i> —The encrypted hexadecimal key.
Required Privilege Level	Crypto Officer—To add and view this statement in the configuration.

key (MACsec)

Syntax	<code>key <i>key-string</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i> security-association <i>security-association-number</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specifies the static security key to exchange to enable MACsec using static secure association key (SAK) security mode.</p> <p>The key string is a 32-digit hexadecimal number. The key string and the security association must match on both sides of an Ethernet connection to secure traffic using MACsec when enabling MACsec using SAK security mode.</p> <p>You must configure at least two security associations with unique security association numbers and key strings to enable MACsec using static SAK security mode. MACsec initially establishes a secure connection when a security association number and key match on both ends of an Ethernet link. After a certain number of Ethernet frames are securely transmitted across the Ethernet link, MACsec automatically rotates to a new security association with a new security association number and key to maintain the secured Ethernet link. This rotation continues each time a certain number of Ethernet frames are securely transmitted across the secured Ethernet link, so you must always configure MACsec to have at least two security associations.</p>
Default	This statement does not have a default value.
Options	<i>key-string</i> —Specifies the key to exchange with the other end of the link on the secure channel. The <i>key-string</i> is a 32-digit hexadecimal string that is created by the user.
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

key-chain (Security)

Syntax	<pre>key-chain <i>key-chain-name</i> { description <i>text-string</i>; key <i>key</i> { algorithm (md5 hmac-sha-1); options (basic isis-enhanced); key-name <i>authentication-key-name</i>; secret <i>secret-data</i>; start-time <i>yyyy-mm-dd.hh:mm:ss</i>; } tolerance <i>seconds</i>; }</pre>
Hierarchy Level	[edit security authentication-key-chains]
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Statement introduced in Junos OS Release 17.4.</p>
Description	Create the key-chain configuration for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.
Options	<p>key-chain-name—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>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • authentication-key-chains on page 677 • <i>Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols</i> • <i>Example: Configuring BFD Authentication for Securing Static Routes</i> • <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

key-server-priority (MACsec)

Syntax	<code>key-server-priority <i>priority-number</i>;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> mka]</code>
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specifies the key server priority used by the MACsec Key Agreement (MKA) protocol to select the key server when MACsec is enabled using static connectivity association key (CAK) security mode.</p> <p>The switch with the lower <i>priority-number</i> is selected as the key server.</p> <p>If the <i>priority-number</i> is identical on both sides of a point-to-point link, the MKA protocol selects the device with the lower MAC address as the key server.</p>
Default	The default key server priority number is 16.
Options	<p><i>priority-number</i>—Specifies the MKA server election priority number.</p> <p>The <i>priority-number</i> can be any number between 0 and 255. The lower the number, the higher the priority.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

key-server-priority (MACsec for MX Series)

Syntax	<code>key-server-priority <i>priority-number</i>;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> mka]</code>
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specifies the key server priority used by the MACsec Key Agreement (MKA) protocol to select the key server when MACsec is enabled using static connectivity association key (CAK) security mode.</p> <p>The switch with the lower <i>priority-number</i> is selected as the key server.</p> <p>If the <i>priority-number</i> is identical on both sides of a point-to-point link, the MKA protocol selects the device with the lower MAC address as the key server.</p>
Default	The default key server priority number is 16.
Options	<p><i>priority-number</i>—Specifies the MKA server election priority number.</p> <p>The <i>priority-number</i> can be any number between 0 and 255. The lower the number, the higher the priority.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

ldap-url

Syntax	<code><ldap-url <i>url-name</i>>;</code>
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series,
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.
Options	<i>url-name</i> —Name of the LDAP URL.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying an LDAP URL on page 179


level

Syntax	<code>level <i>level</i>;</code>
Hierarchy Level	<code>[edit ethernet-switching-options storm-control interface (all <i>interface-name</i>)]</code>
Release Information	Statement introduced in JUNOS Release 9.1 for EX Series switches. Statement deprecated in JUNOS Release 9.5 for EX Series switches. Statement reinstated in JUNOS Release 11.4 for EX Series switches.
Description	For interfaces that are enabled for storm control, configure the storm control level as a percentage of the combined traffic streams that are subject to storm control on that interface.
Default	When storm control is enabled on an interface, the default storm control level is 80 percent of the combined traffic streams that are subject to storm control on that interface.
Options	level —Percentage of the combined traffic streams that are subject to storm control on that interface. Range: 0 through 100 percent Default: 80 percent
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• bandwidth on page 681• Configuring Autorecovery for Port Security Events on page 635• Understanding Storm Control on page 622

lifetime-seconds (Security)


Syntax	<lifetime-seconds <i>seconds</i> >;
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	(Optional) Configure the lifetime of IKE or IPsec SA. When the SA expires, it is replaced by a new SA (and SPI) or terminated.
Options	<i>seconds</i> —Lifetime, in seconds. Range: 180 through 86,400
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Lifetime for an IKE SA • Configuring the Lifetime for an IPsec SA on page 48

light-weight-dhcpv6-relay

Syntax	lightweight-dhcpv6-relay;
Hierarchy Level	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options]
Release Information	Statement introduced in Junos OS Release 16.1R3 for EX Series switches.
Description	<p>Configure a Lightweight DHCPv6 Relay Agent (LDRA) to insert relay agent information in messages sent from a DHCPv6 client to a server or other relay agent on the same IPv6 link. The LDRA acts as a relay agent, but without performing the routing function necessary to forward messages to a server or relay agent that resides on a different IPv6 link.</p> <p>When the LDRA receives a DHCPv6 Solicit message from a client, it encapsulates that message within a DHCPv6 Relay-Forward message, which it then forwards to the server or to another relay agent. Before it forwards the Relay-Forward message, the LDRA can also insert DHCPv6 options in the message. These options contain information that the server uses to assign IP addresses, prefixes, and other configuration parameters for the client.</p> <p>You must configure LDRA if you configure the following DHCPv6 options at the [edit vlan <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options] hierarchy level:</p> <ul style="list-style-type: none"> • option-16 (Vendor ID)—Option 16 provides the server with information about the vendor that manufactured the hardware on which the DHCPv6 client is running. Option 16 is the DHCPv6 equivalent of the vendor-id suboption of DHCP option 82. • option-18 (Interface ID)—A unique identifier for the interface on which the client DHCPv6 packet is received. Suboptions can be configured to include a prefix with the interface ID or to change the type of information used to identify the interface. Option 18 is the DHCPv6 equivalent of the circuit-id suboption of DHCP option 82. • option-37 (Remote ID)—A unique identifier for the remote host. Suboptions can be configured to include a prefix with the remote ID or to change the interface portion of the ID. Option 37 is the DHCPv6 equivalent of the remote-id suboption of DHCP option 82. <p> NOTE: Option 18 is mandatory in Relay-Forward messages and is included even if it is not explicitly configured. However, suboptions of option 18 are included in Relay-Foward messages only if they are configured using the option-18 CLI statement at the [edit vlan <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options] hierarchy level.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Using Lightweight DHCPv6 Relay Agent \(LDRA\) on page 379](#)
 - [no-option18 on page 889](#)
 - [no-dhcpv6-options on page 879](#)

local

Syntax	<pre>local <i>certificate-name</i> { <i>certificate-key-string</i>; load-key-file <i>URL filename</i>; }</pre>
Hierarchy Level	[edit security certificates]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.</p>
	<p> NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.</p>
Options	<p><i>certificate-key-string</i>—String of alphanumeric characters that constitute the private key and certificate.</p> <p><i>certificate-name</i>—Name that uniquely identifies the certificate.</p> <p><i>load-key-file URL filename</i>—File that contains the private key and certificate. It can be one of two types of values:</p> <ul style="list-style-type: none"> • Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router's or switch's local disk) • URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Importing SSL Certificates for Junos XML Protocol Support on page 209

local-certificate (Security)

Syntax	<code>local-certificate <i>certificate-filename</i>;</code>
Hierarchy Level	<code>[edit security ike policy <i>ike-peer-address</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the certificate filename from which to read the local certificate.
Options	<i>certificate-filename</i> —File from which to read the local certificate.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Policy for Digital Certificates for an ES PIC on page 182

local-key-pair

Syntax	<code>local-key-pair <i>private-public-key-file</i>;</code>
Hierarchy Level	<code>[edit security ike policy <i>ike-peer-address</i>]</code>
Release Information	Statement introduced before Junos 7.4.
Description	Specify private and public keys.
Options	<i>private-public-key-file</i> —Specify the file from which to read the private and public key pair.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Policy for Digital Certificates for an ES PIC on page 182

local-traffic-selector

Syntax	<pre>local-traffic-selector { (ipv4-prefix <i>ipv4-prefix</i> ipv6-prefix <i>ipv6-prefix</i>); port <i>port</i>; protocol <i>protocol</i>; }</pre>
Hierarchy Level	[edit security host-vpn connections <i>connection-name</i> children <i>child-name</i>]
Release Information	Statement introduced in Junos OS Evolved Release 18.3R1.
Description	Configure the local IPsec traffic to be protected by the child security association. A traffic selector is a traffic filter that defines and identifies the traffic flow permitted between two systems (a specified pair of local and remote addresses) that have IPsec protection.
Options	<p>(ipv4-prefix <i>ipv4-prefix</i> ipv6-prefix <i>ipv6-prefix</i>)—Specify traffic to be protected by the child security association using either IPv4 or IPv6 with a prefix. The prefix allows for specifying more general traffic.</p> <p>port <i>port</i>—Specify the port to protect by number or name. For example, port 21 and port ftp refer to the same port.</p> <p>protocol <i>protocol</i>—Specify the protocol to protect by number or name. For example, protocol 6 and protocol tcp refer to the same protocol.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>


location

Syntax	<code>location <i>local_pathname</i> <i>remote_URL</i>;</code>
Hierarchy Level	[edit ethernet-switching-options secure-access-port dhcp-snooping-file]
Release Information	Statement introduced in Junos OS Release 12.1 for the QFX Series.
Description	Specify either a local pathname or a remote URL as the location in which to store the DHCP snooping database.
Options	<p><i>local_pathname</i> <i>remote_URL</i> —Location for storing the DHCP snooping database.</p> <ul style="list-style-type: none"> • <i>local_pathname</i> —Use <i>/path</i> to store the database on a local switch. • <i>remote_URL</i> —Use <code>ftp://ip-address</code> or <code>ftp://hostname/path</code> to store the database at a remote location.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>

location (DHCP Snooping Database)

Syntax	<pre>location (<i>local_pathname</i> <i>remote_url</i>); <i>timeout</i> <i>seconds</i>; <i>write-interval</i> <i>seconds</i>; }</pre>
Hierarchy Level	<pre>[edit ethernet-switching-options secure-access-port dhcp-snooping-file]; [edit ethernet-switching-options secure-access-port dhcpv6-snooping-file]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.4 for EX Series switches.</p> <p>Support at the [edit ethernet-switching-options secure-access-port dhcpv6-snooping-file] hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.</p>
Description	<p>Configure IP-MAC address bindings to persist through switch reboots by specifying a location in which to store the DHCP snooping database. When specifying the location for the DHCP snooping database, you must also specify how frequently the switch writes (write-interval) the database entries into the DHCP snooping database file.</p> <p>If you choose to store the DHCP snooping database on a remote FTP site, you might want to specify the time (timeout) that the switch waits for a remote system to respond when the DHCP snooping database is stored on a remote FTP site. This is optional.</p>
Options	<p><i>local_pathname</i> <i>remote_url</i></p> <ul style="list-style-type: none"> • <i>local_pathname</i>—Use <i>/path</i> to store the database file on the local switch. • <i>remote_url</i>—Use ftp://ip-address or ftp:// hostname/path to store the database on a remote FTP site.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Persistent Bindings in the DHCP or DHCPv6 (non-ELS) on page 383 • Understanding DHCP Snooping (non-ELS) on page 393

logical-interface (DDoS Flow Detection)

Syntax	<code>logical-interface (<i>flow-bandwidth</i> <i>flow-control-mode</i> <i>flow-detection-mode</i>)</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers. Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure flow bandwidth, flow control mode, or flow detection mode for flow detection at the logical interface flow aggregation level for the packet type.
Options	<p><i>flow-bandwidth</i>—Bandwidth for the flow at the logical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth] hierarchy level.</p> <p>Default: 200 packets per second</p> <p>Range: 1 through 30,000 packets per second</p> <p><i>flow-control-mode</i>—Mode for how traffic in the detected flow is controlled at the logical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control] hierarchy level.</p>
	<p> NOTE: The configuration at this level overrides the global configuration using the flow-level-control statement at the [edit system ddos-protection global] hierarchy level.</p>
	<ul style="list-style-type: none"> • drop—Drop all traffic in flow. • keep—Keep all traffic in flow. • police—Police the traffic to within its allowed bandwidth. <p>Default: drop</p> <p><i>flow-detection-mode</i>—Mode for how flow detection operates at the logical interface level when a policer has been violated. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection] hierarchy level.</p>



NOTE: The configuration at this level overrides the global configuration using the `flow-detection-mode` statement at the `[edit system ddos-protection global]` hierarchy level.

- **automatic**—Search flows at the logical interface level only when a DDoS policer is being violated and only when the flow causing the policer violation is not discovered at the finer flow aggregation level, subscriber. When the suspicious flow is not found at this level, then the search moves to a coarser level of flow aggregation (physical interface). Flows at the logical interface level are subsequently not searched again until the policer is no longer violated at the coarser level, and a subsequent violation occurs that cannot be found at the subscriber level.
- **off**—Disable flow detection at the logical interface level so that flows are never searched at this level.
- **on**—Search flows at the logical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

Default: `automatic`

Required Privilege Level	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 575• Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 572• Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 571• Configuring Flow Detection for DDoS Protection
------------------------------	--

mac

Syntax	<code>mac mac-address;</code>
Hierarchy Level	<ul style="list-style-type: none"> For platforms with Enhanced Layer 2 Software (ELS): <pre>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security group <i>group-name</i> interface <i>interface-name</i> static-ip <i>ip-address</i>]</pre> For platforms without ELS: <pre>[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>) static-ip <i>ip-address</i> vlan <i>vlan-name</i>]</pre> For MX Series platforms: <pre>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security group <i>group-name</i> interface <i>interface-name</i> static-ip <i>ip-address</i>]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Hierarchy level <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Hierarchy level <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.</p>
Description	Configure the media access control (MAC) address or hardware address of the device connected to the specified interface.
Options	<i>mac-address</i> —Value (in hexadecimal format) of the address assigned to this device.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Static DHCP IP Addresses for DHCP snooping (non-ELS) on page 405 Configuring Static DHCP IP Addresses for DHCP snooping (ELS) on page 404 Configuring Static DHCP IP Addresses for DHCP snooping (MX routers) on page 406

mac (Option 82)

Syntax	<code>mac;</code>
Hierarchy Level	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 remote-id]</code>
Release Information	Statement introduced in Junos OS Release 13.2 for EX Series switches.
Description	Use the MAC address of the port connected to the DHCP client as the remote-id suboption of DHCP option 82 (also known as the DHCP relay agent information option) in DHCP request packet headers before forwarding or relaying requests to a DHCP server. This suboption provides a trusted identifier for the host system that has forwarded or relayed requests to the server.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting Up DHCP Option 82 on the Switch with No Relay (ELS) on page 439• RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046

mac-address (MACsec)

Syntax	<code>mac-address <i>mac-address</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i> id]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specify a MAC address to enable MACsec using static secure association key (SAK) security mode. The mac-address variables must match on the sending and receiving ends of a link to enable MACsec using static SAK security mode.</p> <p>If you are configuring a MAC address on a secure channel in the outbound direction, you should specify the MAC address of the interface as the mac-address.</p> <p>If you are configuring a MAC address on a secure channel in the inbound direction, you should specify the MAC address of the interface at the other end of the link as the mac-address.</p> <p>You only use this configuration option when you are configuring MACsec using static SAK security mode. This option does not need to be specified when you are enabling MACsec using static connectivity association key (CAK) security mode.</p>
Default	No MAC address is specified in the secure channel, by default.
Options	mac-address —The MAC address, in six groups of two hexadecimal digits.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268


mac-address (MACsec)

Syntax	<code>mac-address mac-address;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i> id]</code>
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specify a MAC address to enable MACsec using static secure association key (SAK) security mode. The mac-address variables must match on the sending and receiving ends of a link to enable MACsec using static SAK security mode.</p> <p>If you are configuring a MAC address on a secure channel in the outbound direction, you should specify the MAC address of the interface as the mac-address.</p> <p>If you are configuring a MAC address on a secure channel in the inbound direction, you should specify the MAC address of the interface at the other end of the link as the mac-address.</p> <p>You only use this configuration option when you are configuring MACsec using static SAK security mode. This option does not need to be specified when you are enabling MACsec using static connectivity association key (CAK) security mode.</p>
Default	No MAC address is specified in the secure channel, by default.
Options	mac-address —The MAC address, in six groups of two hexadecimal digits.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228

mac-limit

Syntax	<pre>mac-limit <i>limit</i> { <action <i>action</i>>; }</pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Specify the number of MAC addresses that can be dynamically added to the MAC address cache for this access interface (port) and the action to be taken if the limit is exceeded.
Default	The default action is drop .
Options	<p>limit—Maximum number of MAC addresses.</p> <p>action <i>action</i>—(Optional) Action to take when the MAC address limit is exceeded:</p> <ul style="list-style-type: none"> • drop—Drop the packet and generate a system log entry. This is the default. • log—Do not drop the packet but generate a system log entry. • none—No action. • shutdown—Disable the interface and generate an alarm. If you configure the switch with the port-error-disable statement, the disabled interface recovers automatically upon expiration of the specified timeout. If this statement is not configured, you can bring up the disabled interfaces by running the clear ethernet-switching port-error command.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing—control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding MAC Limiting and MAC Move Limiting for Port Security • Configuring MAC Limiting (QFX Switches) on page 344 • allowed-mac

mac-limit (Access Port Security)

Syntax	<code>mac-limit <i>limit</i> action <i>action</i>;</code>
Hierarchy Level	<code>[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)],</code> <code>[edit ethernet-switching-options secure-access-port interface <i>interface-name</i>) vlan</code> <code><i>vlan-name</i>],</code>
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Set a limit on the number of MAC addresses that can be added to the Ethernet switching table.</p> <ul style="list-style-type: none"> [edit ethernet-switching options secure-access-port interface]—Set the MAC address learning limit for a specific interface, for a range of interfaces, or for all interfaces on the switch. [edit ethernet-switching options secure-access-port interface <i>interface-name</i> vlan <i>vlan-name</i>]—Set the MAC address learning limit for a specific interface as a member of a specific VLAN (VLAN membership MAC limit).
	<p> NOTE: If you set the MAC address limit on a specific interface as a member of a specific VLAN (VLAN membership MAC limit), the switch drops any additional packets when the VLAN membership MAC limit is exceeded and logs the MAC addresses of those packets. You cannot specify a different action for this specific configuration. If a single interface belongs to more than one VLAN, you can set separate VLAN membership MAC limits for the same interface.</p>
	<p>When you reset the number of MAC addresses, the MAC address table is not automatically cleared. Previous entries remain in the table after you reduce the number of addresses, so you should clear the forwarding table for the specified interface or MAC address. Use the clear ethernet-switching table command to clear the existing MAC addresses from the table.</p>
Default	The default action is drop .
Options	<p>action <i>action</i>—(Optional) Action to take when the MAC address limit for an interface or for all interfaces is exceeded:</p> <ul style="list-style-type: none"> drop—Drop the packet and generate a system log entry. log—Do not drop the packet but generate a system log entry. none—No action.

- **shutdown**—Disable the interface and generate a system log entry. If you have configured the switch with the [port-error-disable](#) statement, the disabled interface recovers automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the [clear ethernet-switching port-error](#) command.

limit—Maximum number of MAC addresses.

Required Privilege Level system—To view this statement in the configuration.
system—control—To add this statement to the configuration.

Related Documentation

- [allowed-mac on page 670](#)
- [clear ethernet-switching table on page 1089](#)
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Example: Protecting against Ethernet Switching Table Overflow Attacks on page 354](#)
- [Example: Protecting against DHCP Starvation Attacks on page 347](#)
- [Configuring MAC Limiting \(non-ELS\) on page 341](#)
- [Configuring MAC Limiting \(J-Web Procedure\) on page 346](#)
- [Configuring Autorecovery for Port Security Events on page 635](#)

mac-list

Syntax `mac-list name {
 mac-addresses;
}`

Hierarchy Level [edit policy-options]

Release Information Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.
Statement introduced in Junos OS Release 16.1 for EX Series switches.

Description Define a list of MAC addresses for use in an IPv6 Router Advertisement (RA) guard policy.

Options **mac-addresses**—List of MAC addresses, one MAC address per line in the configuration.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- [Understanding Prefix Lists for Use in Routing Policy Match Conditions](#)

mac-move-limit

Syntax	<pre>mac-move-limit { limit; <action action packet-action action>; }</pre>
Hierarchy Level	<ul style="list-style-type: none"> For platforms with ELS: <pre>[edit vlans vlan-name switch-options]</pre> For platforms without ELS: <pre>[edit ethernet-switching-options secure-access-port vlan (all vlan-name)]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Hierarchy level <code>[edit vlans vlan-name switch-options]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p>
Description	Specify the number of times a MAC address can move to a new interface (port) in one second and the action to be taken by the switch if the MAC address move limit is exceeded.
Default	If you do not specify mac-move-limit , the default MAC address move limit is unlimited.
Options	<p>limit limit—Maximum number of moves to a new interface per second.</p> <ul style="list-style-type: none"> action action—(Optional) (Available <i>only</i> under the hierarchy level <code>[edit ethernet-switching-options secure-access-port vlan (all vlan-name) mac-move-limit]</code>) Action to take when the MAC address move limit is reached: <ul style="list-style-type: none"> drop—Drop the packet and generate a system log entry. This is the default. log—Do not drop the packet but generate a system log entry. none—No action. shutdown—Logically disable the interface and generate a system log entry. If you have configured the switch with the port-error-disable statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the <code>clear ethernet-switching port-error</code> command. packet-action action—(Optional) (Available <i>only</i> under the hierarchy level, <code>[edit vlans vlan-name switch-options mac-move-limit]</code>) Action to take when the MAC address move limit is reached:



NOTE: There is no default action.

- **drop**—Drop the packet and do not generate an alarm.
- **drop and log**—Drop the packet and generate an alarm, an SNMP trap, or system log entry.
- **log**—Do not drop the packet, but generate an alarm, an SNMP trap, or a system log entry.
- **none**—No action.
- **shutdown**—Logically disable the interface and generate an alarm or an SNMP trap. If you have configured the interface with the [recovery-timeout](#) statement, the disabled interface recovers automatically upon expiration of the specified timeout. If you have not configured the interface for a recovery timeout, you can bring up the disabled interface by running the operational command **clear ethernet-switching recovery-timeout**.

Required Privilege Level system—To view this statement in the configuration.
 system—control—To add this statement to the configuration.

- Related Documentation**
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [Configuring MAC Move Limiting \(ELS\) on page 365 \(ELS\)](#)
 - [Configuring Persistent MAC Learning \(ELS\) on page 337](#)
 - [Configuring Autorecovery for Port Security Events on page 635](#)
 - [Configuring Autorecovery for Port Security Events on page 635](#)

macsec

```

Syntax  macsec {
        connectivity-association connectivity-association-name {
            exclude-protocol protocol-name;
            include-sci;
            mka {
                must-secure;
                key-server-priority priority-number;
                transmit-interval interval;
            }
            no-encryption;
            offset (0|30|50);
            pre-shared-key {
                cak hexadecimal-number;
                ckn hexadecimal-number;
            }
            replay-protect {
                replay-window-size number-of-packets;
            }
            secure-channel secure-channel-name {
                direction (inbound | outbound);
                encryption (MACsec);
                id {
                    mac-address mac-address;
                    port-id port-id-number;
                }
                offset (0|30|50);
                security-association security-association-number {
                    key key-string;
                }
            }
            security-mode security-mode;
        }
        interfaces interface-name {
            connectivity-association connectivity-association-name;
        }
    }

```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description Configure Media Access Control Security (MACsec)..

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related
Documentation**

- [Configuring MACsec on EX, SRX and Fusion Devices on page 228](#)

macsec (MX Series)

```

Syntax  macsec {
        connectivity-association connectivity-association-name {
            cipher-suite encryption-algorithm-name;
            exclude-protocol protocol-name;
            pre-shared-key-chain macsec-pre-shared-key-chain-name
            include-sci;
            mka {
                must-secure;
                key-server-priority priority-number;
                transmit-interval interval;
            }
            no-encryption;
            offset (0|30|50);
            pre-shared-key {
                cak hexadecimal-number;
                ckn hexadecimal-number;
            }
            replay-protect{
                replay-window-size number-of-packets;
            }
            secure-channel secure-channel-name {
                direction (inbound | outbound);
                encryption ;
                id {
                    mac-address mac-address;
                    port-id port-id-number;
                }
                offset (0|30|50);
                security-association security-association-number {
                    key key-string;
                }
            }
            security-mode security-mode;
        }
        interfaces interface-name {
            connectivity-association connectivity-association-name;
        }
    }

```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.

Description Configure Media Access Control Security (MACsec) on MX Series routers.

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation • [Configuring Media Access Control Security \(MACsec\) on MX Series Routers on page 268](#)

manual (Junos OS)

Syntax

```
manual {
  direction (inbound | outbound | bi-directional) {
    authentication {
      algorithm (hmac-md5-96 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    auxiliary-spi auxiliary-spi-value;
    encryption {
      algorithm (des-cbc | 3des-cbc);
      key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
  }
}
```

Hierarchy Level [edit security ipsec [security-association](#)]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define a manual IPsec SA.

Options The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation • [Configuring Manual IPsec Security Associations for an ES PIC on page 39](#)

manual (Junos-FIPS Software)

```
Syntax manual {
    direction (bidirectional | inbound | outbound) {
        protocol esp;
        spi spi-value;
        encryption {
            algorithm 3des-cbc;
            key ascii-text ascii-text-string;
        }
        auxiliary-spi auxiliary-spi-value;
        encryption {
            algorithm 3des-cbc;
            key (ascii-text key | hexadecimal key);
        }
        protocol (esp | bundle);
        spi spi-value;
    }
}
```

Hierarchy Level [edit security ipsec internal security-association]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define a manual security association (SA) for internal Routing Engine-to-Routing Engine communication.

Options The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- [Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 211](#)
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

mark-interface (RA Guard)

Syntax	<code>mark-interface (trusted block);</code>
Hierarchy Level	<code>[edit forwarding-options access-security router-advertisement-guard interface interface-name]</code>
Release Information	Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Statement introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Configure an interface as blocked or trusted for IPv6 Router Advertisement (RA) guard. In an IPv6 deployment, RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. RA guard performs checks on incoming RA messages to make sure that they are sent from legitimate routers. If the sender of the RA message cannot be validated, the RA message is dropped.</p> <p>You can configure the mark-interface statement on an interface to bypass RA guard policy checks on that interface. If an interface is configured as either a trusted interface or a blocked interface, RA messages received on the interface are not subject to inspection by RA guard, even if the interface or VLAN is enabled for RA guard. If the interface is trusted, it forwards all RA messages. If the interface is blocked, it drops all RA messages.</p>
Options	<p>block—Configure an interface as blocked for bypassing inspection of RA messages received on that interface by RA guard. When you configure an interface as blocked, all RA messages received on the interface are dropped.</p> <p>trusted—Configure an interface as trusted for bypassing inspection of RA messages received on that interface by RA guard. When you configure an interface as trusted, all RA messages received on the interface are forwarded.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514

match-list

Syntax	<pre> match-list { match-criteria { (match-all match-any); } prefix-list-name <i>prefix-list-name</i>; source-ip-address-list <i>address-list-name</i>; source-mac-address-list <i>address-list-name</i>; } </pre>
Hierarchy Level	[edit forwarding-options access-security router-advertisement-guard <i>policy</i> <i>policy-name</i> accept]
Release Information	Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Statement introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Configure one or more lists of IPv6 addresses, MAC addresses, or IPv6 address prefixes to be associated with an IPv6 Router Advertisement (RA) guard <i>accept</i> policy.</p> <p>RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in the policy.</p> <p>You can configure match lists in either an accept policy or a discard policy. When RA guard is enabled by using an accept policy, RA messages that match the conditions defined in the policy are forwarded, and RA messages that do not match the conditions are dropped. When RA guard is enabled by using a discard policy, RA messages that match the conditions are dropped, and RA messages that do not match the conditions are forwarded.</p> <p>You can associate match lists or match conditions (see match-option) with an accept policy. You can configure match lists that be associated with an accept policy by using the match-list statement. The lists configured by using the match-list statement can contain IPv6 addresses, MAC addresses, or IPv6 address prefixes. RA guard examines the source address or address prefix. You configure the lists at the [edit policy-options] hierarchy level by using the prefix-list option for an IPv6 address or address prefix list, and mac-list for a MAC address list.</p>
Options	<p>match-all—Configure the RA guard policy so that a received RA message is accepted only if it matches criteria in all of the lists configured under match-list; otherwise, the message is discarded.</p> <p>match-any—Configure the RA guard policy so that a received RA message is accepted if it matches criteria in any of the lists configured under match-list; otherwise, the message is discarded.</p>

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Stateless IPv6 Router Advertisement Guard on page 517• Configuring Stateful IPv6 Router Advertisement Guard on page 514

match-option

Syntax	<pre>match-option { hop-limit { (maximum minimum) value; } managed-config-flag; other-config-flag; router-preference maximum (high low medium); }</pre>
Hierarchy Level	[edit forwarding-options access-security router-advertisement-guard policy <i>policy-name</i> accept]
Release Information	Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Statement introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Configure one or more parameters such as hop-count limit, managed configuration flag, other configuration flag, or router preference priority as the match condition to be associated with an IPv6 Router Advertisement (RA) guard <i>accept</i> policy.</p> <p>RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in the policy.</p> <p>You can associate match lists (see match-list) or match conditions with an accept policy. You can configure match conditions by using the match-option statement in an RA guard accept policy. When RA guard is enabled by using an accept policy, any RA messages that match the conditions defined in the policy are forwarded, and RA messages that do not match the conditions are dropped.</p>
Options	<p>hop-limit—Configure the RA guard policy to verify the minimum or maximum hop count for an incoming RA message. Use maximum to set a maximum hop count, or minimum to set a minimum hop count.</p> <p>managed-config-flag—Configure the RA guard policy to verify that the managed address configuration flag of an incoming RA message is set. When the managed address configuration flag is set, it indicates that addresses are available for allocation by Dynamic Host Configuration Protocol version 6 (DHCPv6).</p> <p>other-config-flag—Configure the RA guard policy to verify that the other configuration flag of an incoming RA message is set. When this flag is set, it indicates that other configuration information is available through DHCPv6. Examples of such information are DNS-related information or information on other servers within the network.</p> <p>router-preference-maximum—Configure the RA guard policy to verify that the default router preference parameter value of an incoming RA message is lower than or equal</p>

to a specified limit. The default router preference value improves the ability of IPv6 hosts to select a default router to reach a remote destination when the host has multiple routers on its default router list. Use **high**, **medium**, or **low** to set the maximum preference.

Required Privilege Level	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514

maximum-certificates

Syntax	<code>maximum-certificates <i>number</i>;</code>
Hierarchy Level	[edit security certificates]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>(Encryption interface on M Series and T Series routers and EX Series switches only)</p> <p>Configure the maximum number of peer digital certificates to be cached.</p>
Options	<p><i>number</i>—Maximum number of peer digital certificates to be cached.</p> <p>Range: 64 through 4,294,967,295 peer certificates</p> <p>Default: 1024 peer certificates</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Maximum Number of Peer Certificates on page 181


mka

Syntax	<pre>mka { must-secure; key-server-priority <i>priority-number</i>; transmit-interval <i>interval</i>; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	Specify parameters for the MACsec Key Agreement (MKA) protocol.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228


mka (MX Series)

Syntax	<pre>mka { must-secure; key-server-priority <i>priority-number</i>; transmit-interval <i>interval</i>; eapol-address (pae provider-bridge lldp-multicast); }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers. Option eapol-address introduced in Junos OS Release 18.3R1 for MX Series routers.
Description	Specify parameters for the MACsec Key Agreement (MKA) protocol.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268 • <i>eapol-address</i>

mode (IKE)

Syntax	<code>mode (aggressive main);</code>
Hierarchy Level	<code>[edit security ike policy <i>ike-peer-address</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the IKE policy mode.
	<div>  NOTE: IKEv2 protocol does not negotiate using mode configuration. </div>
Default	main
Options	<p>aggressive—Take half the number of messages of main mode, has less negotiation power, and does not provide identity protection.</p> <p>main—Use six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Policy for Preshared Keys on page 44

mode (IPsec)

Syntax	<code>mode (transport tunnel);</code>
Hierarchy Level	<code>[edit security ipsec security-association name]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the mode for the IPsec security association.
Default	tunnel
Options	<p>transport—Protect traffic when the communication endpoint and cryptographic endpoint are the same. The data portion of the IP packet is encrypted, but the IP header is not. Virtual Private Network (VPN) gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications.</p> <p>tunnel—Protect traffic using preshared keys with IKE to authenticate peers or digital certificates with IKE to authenticate peers.</p>
<div>  <p>NOTE: The Junos OS supports only encapsulating security payload (ESP) when you use tunnel mode.</p> <p>In transport mode, the Junos OS does not support authentication header (AH) and ESP header bundles.</p> <p>In transport mode, the Junos OS supports only Border Gateway Protocol (BGP).</p> </div>	
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Using IPsec to Protect BGP Traffic • Configuring IPsec Tunnel Mode on page 38


multicast

Syntax	<code>multicast;</code>
Hierarchy Level	[edit ethernet-switching-options storm-control interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 11.2 for EX Series switches.
Description	Enable storm control for all multicast traffic (both registered multicast and unregistered multicast) for the specified interface or for all interfaces.
Default	<ul style="list-style-type: none">• On EX2200, EX3200, and EX4200 switches—Storm control does not apply to multicast traffic by default.• On EX4500 and EX8200 switches—Storm control is enabled for multicast traffic.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling and Disabling Storm Control (non-ELS) on page 626

must-secure

Syntax	<code>must-secure;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> mka]</code>
Release Information	Statement introduced in Junos OS Release 14.1X53-D10. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specifies that all traffic travelling on the MACsec-secured link must be MACsec-secured to be forwarded onward.</p> <p>When the must-secure option is enabled, all traffic that is not MACsec-secured that is received on the interface is dropped.</p> <p>When the must-secure option is disabled, all traffic from devices that support MACsec is MACsec-secured while traffic received from devices that do not support MACsec is forwarded through the network.</p> <p>The must-secure option is particularly useful in scenarios where multiple devices, such as a phone and a PC, are accessing the network through the same Ethernet interface. If one of the devices supports MACsec while the other device does not support MACsec, the device that doesn't support MACsec can continue to send and receive traffic over the network—provided the must-secure option is disabled—while traffic to and from the device that supports MACsec is MACsec-secured. In this scenario, traffic to the device that is not MACsec-secured must be VLAN-tagged.</p>
Default	The must-secure option is disabled.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

neighbor-discovery-inspection

Syntax	<code>neighbor-discovery-inspection;</code>
Hierarchy Level	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security];</code> <code>[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>)]</code>
Release Information	Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches. Support at the <code>[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>)]</code> hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches. Statement introduced in Junos OS Release 17.2R1 for the QFX Series.
Description	<p>Perform dynamic IPv6 neighbor discovery inspection on the specified VLAN.</p> <p>When neighbor discovery inspection is configured, the switch inspects IPv6 packets with neighbor discovery messages and validates them against the DHCPv6 binding table. The source IP address and source MAC address of each packet are checked against the table, and if a valid match is not found, the packet is dropped.</p> <hr/> <div>  <p>NOTE: If you configure the <code>neighbor-discovery-inspection</code> statement at the <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> hierarchy level, DHCPv6 snooping is automatically enabled for the specified VLAN.</p> <p>See “IPv6 Neighbor Discovery Inspection” on page 509 for more information about this configuration.</p> <p>If you configure the <code>neighbor-discovery-inspection</code> statement at the <code>[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>)]</code> hierarchy level, you must also enable DHCPv6 snooping for the specified VLAN or VLANs.</p> </div> <hr/>
Default	Disabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Port Security (ELS) on page 9 • Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 492

next-hop-group (Unknown Unicast Forwarding)

Syntax

```
next-hop-group group-name {
  group-type {
    layer-2;
  }
  interface interface-name {
    next-hop address;
  }
  next-hop-subgroup subgroup-name {
    interface interface-name;
  }
}
```

Hierarchy Level [edit [forwarding-options](#)]

Release Information Statement introduced in Junos OS Release 14.2 for EX Series switches.

Description Configure a next-hop group to forward unknown unicast packets to a specific interface or interfaces.

Options *group-name*—Name of the next-hop group.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Unknown Unicast Forwarding \(ELS\) on page 614](#)
- [Configuring Mirroring on EX9200 Switches to Analyze Traffic \(CLI Procedure\)](#)

no-allowed-mac-log

Syntax	no-allowed-mac-log;
Hierarchy Level	[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify that the switch does not log messages when it receives packets from invalid MAC addresses on an interface that has been configured for particular (allowed) MAC addresses.
Default	The switch logs messages when it receives packets from invalid MAC addresses on an interface that has been configured for particular (allowed) MAC addresses.
Required Privilege Level	system—To view this statement in the configuration. system—control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• allowed-mac on page 670• Example: Configuring Port Security (non-ELS) on page 15• Example: Protecting Against DHCP Snooping Database Attacks on page 415• Example: Protecting against DHCP Starvation Attacks on page 347• Configuring MAC Limiting (non-ELS) on page 341

no-broadcast

Syntax	no-broadcast;
Hierarchy Level	<ul style="list-style-type: none"> For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): <pre>[edit forwarding-options storm-control-profiles profile-name all]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p> <p>Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p>
Description	Disable storm control for broadcast traffic for the specified interface or for all interfaces.
Default	<ul style="list-style-type: none"> On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control on broadcast, multicast, or unknown-unicast traffic. On EX4300 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. You can selectively disable storm control on any type of traffic. On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. On EX8200 switches, you can selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic. On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control for each type of traffic individually. On EX9200 switches—Storm control is not enabled by default. On MX Series routers—Storm control is not enabled by default.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Configuring Autorecovery for Port Security Events on page 635](#)
 - [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches](#)
 - [Example: Using Storm Control to Prevent Network \(MX Routers\) on page 641](#)
 - [Enabling and Disabling Storm Control \(non-ELS\) on page 626](#)
 - [Enabling and Disabling Storm Control \(ELS\) on page 630](#)

no-dhcp-snooping

Syntax	no-dhcp-snooping;
Hierarchy Level (EX Series, QFX Series)	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]
Hierarchy Level (MX Series)	[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX series. Hierarchy level [edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 14.1 for the MX Series.
Description	Disable DHCP snooping for the specified VLAN or bridge domain.



NOTE: Explicitly disabling DHCP snooping also disables any other port security features that you have enabled under [edit vlans *vlan-name* forwarding-options **dhcp-security**], including dynamic ARP inspection (DAI) and IP source guard for the specified VLAN or bridge domain.

There is no configuration statement that explicitly enables DHCP snooping.

Default DHCP snooping is not enabled.



NOTE: Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style and MX Series routers do not have a configuration statement that explicitly enables DHCP snooping.

DHCP snooping is enabled automatically by Junos OS if any of the following is configured at the [edit vlans *vlan-name* forwarding-options **dhcp-security**] hierarchy level for EX Series and QFX Series switches or at the [edit bridge-domains *bridge-domain-name* forwarding-options **dhcp-security**] for MX Series routers:

- DAI
- IP source guard
- Static IP
- DHCP option 82

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Understanding DHCP Snooping \(non-ELS\) on page 393](#)

no-dhcp-trusted

Syntax (dhcp-trusted | no-dhcp-trusted);

Hierarchy Level [edit [ethernet-switching-options](#) secure-access-port [interface \(Access Port Security\)](#) (all | *interface-name*)]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Port security features, such as DHCP snooping and dynamic ARP inspection inspect packets only on untrusted interfaces.

Allow or deny DHCP responses from the specified interfaces (ports) or all interfaces.

- **dhcp-trusted**—Allow DHCP responses.
- **no-dhcp-trusted**—Deny DHCP responses.

Default Trusted for trunk ports, untrusted for access ports.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- [Understanding How to Protect Access Ports from Common Attacks on page 6](#)
- [Understanding and Using Trusted DHCP Servers on page 371](#)

no-dhcpv6-options

Syntax	no-dhcpv6-options;
Hierarchy Level	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security group group-name overrides]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Configure a specific group of one or more access interfaces within the VLAN not to add any DHCPv6 options, even if the VLAN is configured to perform DHCPv6 snooping. DHCPv6 options include option 16, option 18, and option 37.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • dhcpv6-options on page 731 • Understanding DHCP Snooping (ELS) on page 385 • Understanding DHCP Option 82 on page 429

no-dhcpv6-snooping

Syntax	no-dhcpv6-snooping;
Hierarchy Level	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]
Release Information	Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches.
Description	Disable DHCPv6 snooping for the specified VLAN.
Default	<p>DHCPv6 snooping is not enabled by default.</p> <p>There is no configuration statement that explicitly enables DHCPv6 snooping. DHCPv6 snooping is enabled automatically by Junos OS if any port security feature, such as IPv6 neighbor discovery inspection or IPv6 source guard, is configured at the [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] hierarchy level.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding DHCP Snooping (non-ELS) on page 393

no-encryption (MACsec)

Syntax	no-encryption;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Disables MACsec encryption for a connectivity association that is configured to enable MACsec using static connectivity association key (CAK) or dynamic security mode.</p> <p>You can enable MACsec without enabling encryption. If a connectivity association that has not enabled MACsec encryption is associated with an interface, traffic is forwarded across the Ethernet link in clear text. You are, therefore, able to view this unencrypted traffic when you are monitoring the link. The MACsec header is still applied to the packet, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic does not represent a security threat.</p> <p>This command is used to disable encryption when MACsec is configured using static CAK or dynamic security mode only. When MACsec is configuring using static secure association key (SAK) security mode, the encryption setting is managed in the secure channel using the encryption configuration statement.</p>
Default	MACsec encryption is enabled if MACsec is enabled using static CAK or dynamic security mode.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228


no-encryption (MACsec for MX Series)

Syntax	no-encryption;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Disables MACsec encryption for a connectivity association that is configured to enable MACsec using static connectivity association key (CAK) or dynamic security mode.</p> <p>You can enable MACsec without enabling encryption. If a connectivity association that has not enabled MACsec encryption is associated with an interface, traffic is forwarded across the Ethernet link in clear text. You are, therefore, able to view this unencrypted traffic when you are monitoring the link. The MACsec header is still applied to the packet, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic does not represent a security threat.</p> <p>This command is used to disable encryption when MACsec is configured using static CAK or dynamic security mode only. When MACsec is configuring using static secure association key (SAK) security mode, the encryption setting is managed in the secure channel using the encryption configuration statement.</p>
Default	MACsec encryption is enabled if MACsec is enabled using static CAK or dynamic security mode.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268


no-examine-dhcpv6

Syntax	<pre>no-examine-dhcpv6 { forwarding-class class-name; }</pre>
Hierarchy Level	[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	<p>Disable DHCPv6 snooping on all VLANs or on the specified VLAN.</p> <p>The remaining statement is explained separately.</p>
Default	Disabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• examine-dhcpv6 on page 763• Example: Configuring Port Security (non-ELS) on page 15• Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks on page 406• Example: Protecting Against ARP Spoofing Attacks on page 418• Example: Prioritizing Snooped and Inspected Packet on page 423• Enabling DHCP Snooping (non-ELS) on page 400• Enabling DHCP Snooping (J-Web Procedure)

no-fcoe-trusted

Syntax	no-fcoe-trusted;
Hierarchy Level	Original CLI <pre>[edit ethernet-switching-options secure-access-port interface <i>interface-name</i>]</pre> ELS CLI for Platforms that Support FCoE <pre>[edit vlans <i>vlan-name</i> forwarding-options fip-security interface <i>interface-name</i>]</pre>
	<div>  <p>NOTE: The no-fcoe-trusted configuration statement is in a different hierarchy on the original CLI than on the Enhanced Layer 2 Software (ELS) CLI.</p> </div>
Release Information	Statement introduced in Junos OS Release 10.4 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced for the ELS CLI in Junos OS Release 13.2 for the QFX Series.
Description	<p>Configure the specified 10-Gigabit Ethernet interface not to trust Fibre Channel over Ethernet (FCoE) traffic. If an interface is directly connected to an FCoE device, the interface should not be configured as an FCoE trusted interface. If an interface that you want to connect to an FCoE device has been configured as an FCoE trusted interface, use the no-fcoe-trusted statement to convert the interface to an untrusted interface. Untrusted interfaces can perform FIP snooping to provide access security for FCoE traffic.</p> <p>However, if an interface is connected to another switch such as an FCoE forwarder (FCF) or a transit switch, you can configure the interface as trusted so that the interface forwards FCoE traffic from the switch to the FCoE devices without installing FIP snooping filters.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>show fip snooping</i> • <i>Example: Configuring an FCoE Transit Switch</i> • <i>Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch</i> • <i>Configuring VN2VF_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch</i>

no-flow-logging (DDoS Flow Detection)

Syntax	no-flow-logging;
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i>]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers. Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Disable automatic logging of flow detection culprit flow events (flow reports) for the packet type. <div> NOTE: You can disable logging of suspicious flow events (violation reports) with the <code>disable-logging</code> statement at the [edit system ddos-protection global hierarchy level].</div>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 574• Configuring Flow Detection for DDoS Protection

no-gratuitous-arp-request

Syntax	no-gratuitous-arp-request;
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the switch not to respond to gratuitous ARP requests. You can disable responses to gratuitous ARP requests on Layer 2 Ethernet switching interfaces, and integrated routing and bridging (IRB) interfaces or routed VLAN interfaces (RVIs). (On EX Series switches that use Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, the feature is known as an IRB interface. On EX Series switches that use Junos OS that does not support ELS, the feature is known as an RVI.)
Default	Gratuitous ARP responses are enabled on all Ethernet switching interfaces, and IRB interfaces or RVIs.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Proxy ARP on an EX Series Switch</i> • <i>Configuring Proxy ARP on Switches</i> • <i>Configuring Proxy ARP on Devices with ELS Support</i>

no-gratuitous-arp-request

Syntax	no-gratuitous-arp-request;
Hierarchy Level	[edit interfaces <i>interface-name</i>], [edit interfaces interface-range <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Configure the switch not to respond to gratuitous ARP requests. You can disable responses to gratuitous ARP requests on both Layer 2 Ethernet switching interfaces and routed VLAN interfaces (RVIs).
Default	Gratuitous ARP responses are enabled on all Ethernet switching interfaces and RVIs.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring IRB Interfaces on Switches</i>

no-multicast

Syntax	no-multicast;
Hierarchy Level	<ul style="list-style-type: none"> For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): <pre>[edit forwarding-options storm-control-profiles profile-name all]</pre> For platforms without ELS: <pre>[edit ethernet-switching-options storm-control interface (all interface-name)]</pre>
Release Information	<p>Statement introduced in Junos OS Release 10.3 for EX Series switches.</p> <p>Hierarchy level <code>[edit forwarding-options]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p>
Description	Disable storm control for all multicast traffic (both registered multicast and unregistered multicast) for the specified interface or for all interfaces.
Default	<ul style="list-style-type: none"> On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. On EX4300 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. You can selectively disable storm control on any type of traffic. On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. On EX8200 switches, you can selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic. On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control for each type of traffic individually. On EX9200 switches—Storm control is not enabled by default. On MX Series routers—Storm control is not enabled by default.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [no-registered-multicast on page 891](#)
- [no-unregistered-multicast on page 894](#)
- [Enabling and Disabling Storm Control \(non-ELS\) on page 626](#)
- [Enabling and Disabling Storm Control \(ELS\) on page 630](#)

no-option16

Syntax no-option16;

Hierarchy Level [edit vlans *vlan-name* forwarding-options [dhcp-security group group-name overrides](#)]

Release Information Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Configure a specific group of one or more access interfaces within the VLAN not to transmit DHCPv6 option 16 information, even if the VLAN is configured to perform DHCPv6 snooping. Option 16 information that has already been added by a DHCPv6 client will be forwarded as is.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [option-16 on page 898](#)
- [Understanding DHCP Snooping \(ELS\) on page 385](#)
- [Understanding DHCP Option 82 on page 429](#)

no-option18

Syntax	no-option18;
Hierarchy Level	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security group group-name overrides]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Configure a specific group of one or more access interfaces within the VLAN <i>not</i> to transmit DHCP option 18 information, even if the VLAN is configured to perform DHCPv6 snooping.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • option-18 on page 899 • Understanding DHCP Option 82 on page 429 • Understanding DHCP Snooping (ELS) on page 385

no-option37

Syntax	no-option37;
Hierarchy Level	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security group group-name overrides]
Release Information	Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches.
Description	Configure a specific group of one or more access interfaces within the VLAN <i>not</i> to transmit DHCP option 37 information, even if the VLAN is configured to perform DHCPv6 snooping.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • option-37 on page 901 • Understanding DHCP Option 82 on page 429 • Understanding DHCP Snooping (non-ELS) on page 393

no-option82

Syntax	no-option82;
Hierarchy Level (EX Series, QFX Series)	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security group group-name overrides]
Hierarchy Level (MX Series)	[edit bridge-domains <i>bridge-domain-name</i> forwarding-options group group group-name overrides]
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX series. Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	Configure a specific group of one or more access interfaces within the VLAN or bridge domain <i>not</i> to transmit DHCP option 82 information, even if the VLAN or bridge domain is configured to use option 82.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• option-82 on page 903• Setting Up DHCP Option 82 on the Switch with No Relay (ELS) on page 439• Understanding DHCP Option 82 on page 429• Understanding DHCP Snooping (non-ELS) on page 393

no-registered-multicast

Syntax	no-registered-multicast;
Hierarchy Level	<ul style="list-style-type: none"> For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): <pre>[edit forwarding-options storm-control-profiles profile-name all]</pre> For platforms without ELS: <pre>[edit ethernet-switching-options storm-control interface (all interface-name)]</pre>
Release Information	<p>Statement introduced in Junos OS Release 10.3 for EX Series switches.</p> <p>Hierarchy level <code>[edit forwarding-options]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>(EX8200 switches only) Disable storm control for registered multicast traffic for the specified interface or for all interfaces.</p> <p>(EX4300 and EX9200 switches only) Exclude storm control for registered multicast traffic from a storm control profile.</p> <p>(MX Series routers only) Exclude storm control for registered multicast traffic from a storm control profile.</p>
Default	<p>EX4300 and EX8200 switches—Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic. The default storm control level is 80 percent of the available bandwidth used by the combined applicable traffic streams.</p> <p>EX9200 switches—Storm control is not enabled by default.</p> <p>MX Series routers—Storm control is not enabled by default.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> no-multicast on page 887 no-unregistered-multicast on page 894 Understanding Storm Control on page 622 Understanding Storm Control on page 622

no-unknown-unicast

Syntax	no-unknown-unicast;
Hierarchy Level	<ul style="list-style-type: none"> For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): <pre>[edit forwarding-options storm-control-profiles profile-name all]</pre> For platforms without ELS: <pre>[edit ethernet-switching-options storm-control interface (all interface-name)]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p> <p>Hierarchy level [edit forwarding-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p>
Description	Disable storm control for unknown unicast traffic for the specified interface or for all interfaces.
Default	<ul style="list-style-type: none"> On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control on broadcast, multicast, or unknown-unicast traffic. On EX4300 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. You can selectively disable storm control on any type of traffic. On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. On EX8200 switches, you can selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic. On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control for each type of traffic individually. On EX9200 switches—Storm control is not enabled by default.

- MX Series routers—Storm control is not enabled by default.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Autorecovery for Port Security Events on page 635](#)
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- [Example: Using Storm Control to Prevent Network \(MX Routers\) on page 641](#)
- [Enabling and Disabling Storm Control \(non-ELS\) on page 626](#)
- [Enabling and Disabling Storm Control \(ELS\) on page 630](#)

no-unregistered-multicast

Syntax	no-unregistered-multicast;
Hierarchy Level	<ul style="list-style-type: none"> For platforms with Enhanced Layer 2 Software (ELS) (EX Series switches and MX Series routers): <pre>[edit forwarding-options storm-control-profiles profile-name all]</pre> For platforms without ELS: <pre>[edit ethernet-switching-options storm-control interface (all interface-name)]</pre>
Release Information	<p>Statement introduced in Junos OS Release 10.3 for EX Series switches.</p> <p>Hierarchy level <code>[edit forwarding-options]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>(EX8200 switches only) Disable storm control for unregistered multicast traffic for the specified interface or for all interfaces.</p> <p>(EX4300 and EX9200 switches only) Exclude storm control for unregistered multicast traffic from a storm control profile.</p> <p>(MX Series routers) Exclude storm control for unregistered multicast traffic from a storm control profile.</p>
Default	<p>EX4300 and EX8200 switches—Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic. The default storm control level is 80 percent of the available bandwidth used by the combined applicable traffic streams.</p> <p>EX9200 switches—Storm control is not enabled by default.</p> <p>MX Series routers—Storm control is not enabled by default.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> no-multicast on page 887 no-registered-multicast on page 891 Understanding Storm Control on page 622 Understanding Storm Control on page 622

offset

Syntax	<code>offset (0 30 50);</code>
Hierarchy Level	<code>[edit security macsec connectivity-association connectivity-association-name] [edit security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name]</code>
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Configure a confidentiality offset for MACsec. When MACsec is enabled with encryption, the confidentiality offset specifies a number of octets in an Ethernet frame that are sent in unencrypted plain-text.</p> <p>Per 802.1AE-2006, confidentiality offset is relevant for switch-to-host connections by allowing a system that is incapable of terminating the secure association before distributing the load to perform load balancing across multiple processors based on the first few bytes of packets. Additionally, confidentiality offset can be used to expose IPv4 or IPv6 headers to bump-in-the-wire devices, such as transparent firewalls or monitoring devices.</p> <p>Setting the offset to 30 allows a feature to see the IPv4 header and the TCP/UDP header while encrypting the remaining traffic. Setting the offset to 50 allows a feature to see the IPv6 header and the TCP/UDP header while encrypting the remaining traffic.</p> <p>You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.</p> <p>You configure the offset in the <code>[edit security macsec connectivity-association connectivity-association-name]</code> hierarchy when you are enabling MACsec using static connectivity association key (CAK) or dynamic security mode.</p> <p>You configure the offset in the <code>[edit security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name]</code> hierarchy when you are enabling MACsec using static secure association key (SAK) security mode.</p>
Default	0
Options	0—Specifies that no octets are unencrypted. When you set the offset to 0, all traffic on the interface where the connectivity association or secure channel is applied is encrypted.

30—Specifies that the first 30 octets of each Ethernet frame are unencrypted.



NOTE: In IPv4 traffic, setting the offset to 30 allows a feature to see the IPv4 header and the TCP/UDP header while encrypting the rest of the traffic. An offset of 30, therefore, is typically used when a feature needs this information to perform a task on IPv4 traffic.

50—Specified that the first 50 octets of each Ethernet frame are unencrypted.



NOTE: In IPv6 traffic, setting the offset to 50 allows a feature to see the IPv6 header and the TCP/UDP header while encrypting the rest of the traffic. An offset of 50, therefore, is typically used when a feature needs this information to perform a task on IPv6 traffic.

Required Privilege	admin—To view this statement in the configuration.
Level	admin-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228
------------------------------	--

offset (MX Series)

Syntax	<code>offset (0 30 50);</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i>]</code> <code>[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specifies the number of octets in an Ethernet frame that are sent in unencrypted plain-text when encryption is enabled for MACsec.</p> <p>Setting the offset to 30 allows a feature to see the IPv4 header and the TCP/UDP header while encrypting the remaining traffic. Setting the offset to 50 allows a feature to see the IPv6 header and the TCP/UDP header while encrypting the remaining traffic.</p> <p>You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.</p> <p>You configure the offset in the <code>[edit security macsec connectivity-association <i>connectivity-association-name</i>]</code> hierarchy when you are enabling MACsec using static connectivity association key (CAK) or dynamic security mode.</p> <p>You configure the offset in the <code>[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i>]</code> hierarchy when you are enabling MACsec using static secure association key (SAK) security mode.</p>
Default	0
Options	<p>0—Specifies that no octets are unencrypted. When you set the offset to 0, all traffic on the interface where the connectivity association or secure channel is applied is encrypted.</p> <p>30—Specifies that the first 30 octets of each Ethernet frame are unencrypted.</p>



NOTE: In IPv4 traffic, setting the offset to 30 allows a feature to see the IPv4 header and the TCP/UDP header while encrypting the rest of the traffic. An offset of 30, therefore, is typically used when a feature needs this information to perform a task on IPv4 traffic.

50—Specified that the first 50 octets of each Ethernet frame are unencrypted.



NOTE: In IPv6 traffic, setting the offset to 50 allows a feature to see the IPv6 header and the TCP/UDP header while encrypting the rest of the traffic. An offset of 50, therefore, is typically used when a feature needs this information to perform a task on IPv6 traffic.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Media Access Control Security \(MACsec\) on MX Series Routers on page 268](#)

option-16 (DHCPv6 Snooping)

Syntax

```
option-16 {
    use-string string;
}
```

Hierarchy Level [edit vlans *vlan-name* forwarding-options **dhcp-security** **dhcpv6-options**]

Release Information Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Configure the DHCPv6 Vendor ID option (option 16) to be included in DHCPv6 requests from clients before forwarding them to a DHCPv6 server. Option 16 provides the server with information about the vendor that manufactured the hardware on which the DHCP client is running. When configured, the switch will overwrite any existing option 16 information sent by clients in the DHCPv6 packets.

Option 16 is the DHCPv6 equivalent of the **vendor-id** sub-option of DHCP option 82.

Options **use-string *string***—Define a custom string to be used as the DHCPv6 vendor identifier.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Enabling Dynamic ARP Inspection \(ELS\) on page 451](#)
- [Configuring IP Source Guard \(ELS\) on page 465](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\) on page 439](#)
- [Configuring Static DHCP IP Addresses for DHCP snooping \(ELS\) on page 404](#)

option-18 (DHCPv6 Snooping)

Syntax

```
option-18 {
  prefix {
    host-name;
    logical-system-name;
    routing-instance-name;
    vlan-id;
    vlan-name;
  }
  use-interface-index (device | logical);
  use-interface-description (device | logical);
  use-interface-mac;
  use-interface-name (device | logical);
  use-string string;
}
```

Hierarchy Level [edit vlans *vlan-name* forwarding-options [dhcp-security dhcpv6-options](#)]

Release Information Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Configure the DHCPv6 Relay Agent Interface ID option (option 18) to insert information in DHCPv6 requests from clients before forwarding them to a DHCPv6 server. Option 18 provides information about the port on which the request was received, which the server can use to assign IP addresses, prefixes, and other configuration parameters for the client.

When option 18 is configured, a unique interface ID is inserted into the DHCPv6 packet headers. Suboptions can be configured to include a prefix with the interface ID or to change the type of information used to identify the interface. The default fields included in option 18 are the Juniper Enterprise ID, VLAN, and MAC address of the interface.

Option 18 is the DHCPv6 equivalent of the [circuit-id](#) sub-option of DHCP option 82.



NOTE: DHCPv6 packets that already contain option 18 information when received from a client are dropped by the switch.

Options **use-interface-mac**—Use the MAC address of the interface in the DHCPv6 interface ID.

use-string *string*—Use a custom string in the DHCPv6 interface ID.

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**
- [no-option18 on page 889](#)
 - [no-dhcpv6-options on page 879](#)

option-37 (DHCPv6 Snooping)

Syntax

```
option-37 {
  prefix {
    host-name;
    logical-system-name;
    routing-instance-name;
    vlan-id;
    vlan-name;
  }
  use-interface-index (device | logical);
  use-interface-description (device | logical);
  use-interface-mac;
  use-interface-name (device | logical);
  use-string string;
}
```

Hierarchy Level [edit vlans *vlan-name* forwarding-options **dhcp-security dhcpv6-options**]

Release Information Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Configure the DHCPv6 Relay Agent Remote ID option (option 37) to insert information in DHCPv6 requests from clients before forwarding them to a DHCPv6 server. Option 37 provides information about the remote host, which the server can use to assign IP addresses, prefixes, and other configuration parameters for the client.

When option 37 is configured, a unique remote ID is inserted into the DHCPv6 packet headers. Suboptions can be configured to include a prefix with the remote ID or to change the interface portion of the ID. The default fields included in option 37 are the Juniper Enterprise ID, VLAN, and MAC address of the interface.

Option 37 is the DHCPv6 equivalent of the **remote-id** sub-option of DHCP option 82.



NOTE: DHCPv6 packets that already contain option 37 information when received from a client are dropped by the switch.

Options **use-interface-mac**—Use the MAC address of the interface in the DHCPv6 remote ID.

use-string *string*—Use a custom string in the DHCPv6 remote ID.

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**
- [no-option37 on page 889](#)
 - [no-dhcpv6-options on page 879](#)
 - [Setting Up DHCP Option 82 on the Switch with No Relay \(ELS\) on page 439](#)
 - [Configuring Static DHCP IP Addresses for DHCP snooping \(ELS\) on page 404](#)

no-option-37

Syntax	no-option-37;
Hierarchy Level	[edit ethernet-switching-options secure-access-port vlan <i>vlan-name</i>]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Configure the VLAN <i>not</i> to transmit DHCP option 37 information, even if the VLAN is configured to perform DHCPv6 snooping.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• option-82 on page 903• Understanding DHCP Option 82 on page 429• Understanding DHCP Snooping (non-ELS) on page 393

option-82

Syntax	<pre> option-82 { circuit-id { prefix (host-name routing-instance-name); use-interface-description; use-vlan-id; } remote-id { host-name; mac (Option 82); use-interface-description; use-string string; } vendor-id { use-string string; } } </pre>
Hierarchy Level (EX Series, QFX Series)	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]
Hierarchy Level (MX Series)	[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]
Release Information	<p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1 for the MX Series.</p>
Description	<p>Have the device insert DHCP option 82 (also known as the DHCP relay agent information option) information in the DHCP request packet header of a DHCP request that it receives from a DHCP client connected to one of its interfaces before it forwards or relays that DHCP request to a DHCP server. The server uses the option 82 information, which provides details about the circuit and host the request came from. However, in formulating the reply, the server does not make any changes to the option 82 information in the packet header. The device receives the reply and then removes the DHCP option 82 information before forwarding the reply to the client.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Default	Insertion of DHCP option 82 information is not enabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Setting Up DHCP Option 82 on the Switch with No Relay (ELS) on page 439 • no-option82 on page 890

- [Understanding DHCP Option 82 on page 429](#)
- [Understanding DHCP Snooping \(non-ELS\) on page 393](#)
- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>

options (Security)

Syntax	options (basic isis-enhanced);
Hierarchy Level	[edit security authentication-key-chains key-chain <i>key-chain-name</i> key <i>key</i>]
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	<p>For IS-IS only, configure the protocol transmission encoding format for encoding the message authentication code in routing protocol packets.</p> <p>Because this setting is for IS-IS only, the TCP and the BFD protocol ignore the encoding option configured in the key.</p>
Options	<p>basic—RFC 5304 based encoding. Junos OS sends and receives RFC 5304-encoded routing protocols packets, and drops 5310-encoded routing protocol packets that are received from other devices.</p> <p>isis-enhanced—RFC 5310 based encoding. Junos OS sends RFC 5310-encoded routing protocol packets and accepts both RFC 5304-encoded and RFC 5310-encoded routing protocol packets that are received from other devices.</p> <p>Default: basic</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Hitless Authentication Key Rollover for IS-IS• Understanding Hitless Authentication Key Rollover for IS-IS

overrides (DHCP Security)

Syntax	<pre>overrides { no-dhcpv6-options; no-option16; no-option18; no-option37; no-option82; trusted; untrusted; }</pre>
Hierarchy Level	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security group <i>group-name</i>]
Release Information	<p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Support for the no-option37 option introduced in Junos OS Release 13.2X51-D20 for EX Series switches.</p> <p>Support for the no-dhcpv6-options, no-option16 and no-option18 options introduced in Junos OS Release 14.2 for EX Series switches.</p>
Description	Modify selected DHCP attributes for a group of interfaces that is configured within a specified VLAN.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Enabling a Trusted DHCP Server (ELS) on page 372 • Understanding DHCP Snooping (non-ELS) on page 393 • Understanding DHCP Option 82 on page 429

overrides (DHCP Security for MX Series)

Syntax	<code>overrides (trusted untrusted no-option82);</code>
Hierarchy Level	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security group <i>group-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	Modify selected attributes of a specific interface within a group of interfaces configured within a specified bridge domain.
Options	<p>no-option 82 —The interface specified in this group does not support DHCP option 82.</p> <p>trusted—The interface specified in this group is trusted. DHCP snooping does not apply to the trusted interface. Likewise, DAI and IP source guard—even if they are enabled for the VLAN or bridge domain—do not apply to the interface that is configured with the overrides and the trusted options. Trunk interfaces are trusted by default. Access interfaces are untrusted by default.</p> <p>untrusted— The interface specified in this group is untrusted. Trunk interfaces are trusted by default. Access interfaces are untrusted by default.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring DHCP Option 82 on a Router with Bridge Domain on page 437• Understanding DHCP Option 82 on page 429

packet-action

Syntax `packet-action action;`

Hierarchy Level [edit **bridge-domains** *bridge-domain-name* bridge-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit **bridge-domains** *bridge-domain-name* bridge-options **interface-mac-limit** *limit*],
 [edit logical-systems *logical-system-name* **bridge-domains** *bridge-domain-name* bridge-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit logical-systems *logical-system-name* **bridge-domains** *bridge-domain-name* bridge-options **interface-mac-limit** *limit*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* **bridge-domains** *bridge-domain-name* bridge-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* **bridge-domains** *bridge-domain-name* bridge-options **interface-mac-limit** *limit*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* switch-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* switch-options **interface-mac-limit** *limit*],
 [edit logical-systems *logical-system-name* switch-options **interface-mac-limit** *limit*],
 [edit protocols l2-learning global-mac-limit *limit*],
 [edit routing-instances *routing-instance-name* **bridge-domains** *bridge-domain-name* bridge-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit routing-instances *routing-instance-name* **bridge-domains** *bridge-domain-name* bridge-options **interface-mac-limit** *limit*],
 [edit routing-instances *routing-instance-name* protocols evpn interface-mac-limit (VPLS)],
 [edit routing-instances *routing-instance-name* protocols evpn interface *interface-name* interface-mac-limit (VPLS)],
 [edit routing-instances *routing-instance-name* protocols evpn mac-table-size *limit*],
 [edit routing-instances *routing-instance-name* switch-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit routing-instances *routing-instance-name* switch-options **interface-mac-limit** *limit*],
 [edit switch-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit switch-options **interface-mac-limit** *limit*],
 [edit switch-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit switch-options **interface-mac-limit** *limit*],
 [edit switch-options mac-table-size *limit*],
 [edit switch-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit vlans *vlan-name* switch-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit vlans *vlan-name* switch-options **interface-mac-limit** *limit*],
 [edit vlans *vlan-name* switch-options mac-table-size *limit*]
 [edit vlans *vlan-name* switch-options **interface-mac-limit** *limit*],
 [edit vlans *vlan-name* switch-options interface *interface-name* **interface-mac-limit** *limit*],
 [edit vlans *vlan-name* switch-options mac-table-size *limit*]

Release Information Statement introduced in Junos OS Release 8.4.
 Support for the **switch-options** statement added in Junos OS Release 9.2.
 Support for top-level configuration for the **virtual-switch** type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy

supported this statement only for a VPLS instance or a bridge domain configured within a virtual switch.

Support for logical systems added in Junos OS Release 9.6.

[edit switch-options interface *interface-name* interface-mac-limit *limit*], [edit switch-options interface-mac-limit *limit*], [edit switch-options mac-table-size *limit*], [edit vlans *vlan-name* switch-options interface *interface-name* interface-mac-limit *limit*], [edit vlans *vlan-name* switch-options interface-mac-limit *limit*], and [edit vlans *vlan-name* switch-options mac-table-size *limit*] hierarchy levels introduced in Junos OS Release 12.3R2 for EX Series switches.

Support for EVPNs introduced in Junos OS Release 13.2 on MX Series 5G Universal Routing Platforms.

Support at the [edit switch-options interface *interface-name* interface-mac-limit *limit*] hierarchy level and hierarchy levels under [edit vlans *vlan-name*] introduced in Junos OS Release 13.2X50-D10 for EX Series switches and Junos OS Release 13.2 for the QFX Series.

Description Specify the action taken when packets with new source MAC addresses are received after the MAC address limit is reached. If this statement is not configured, packets with new source MAC addresses are forwarded by default.



NOTE: The `packet-action` statement is not supported on the QFX10002-60C switch.

Default



NOTE: On a QFX Series Virtual Chassis, if you include the shutdown option at the [edit vlans *vlan-name* switch-options interface *interface-name* interface-mac-limit packet-action] hierarchy level and issue the commit operation, the system generates a commit error. The system does not generate an error if you include the shutdown option at the [edit switch-options interface *interface-name* interface-mac-limit packet-action] hierarchy level.

Disabled. The default is for packets for new source MAC addresses to be forwarded after the MAC address limit is reached.

Options **drop**—Drop packets with new source MAC addresses, and do not learn the new source MAC addresses.



NOTE: On QFX10000 switches, if you include the drop option, you cannot configure unicast reverse-path forwarding (URFP) on integrated routing and bridging (IRB) and MAC limiting on the same interface. If you have an MC-LAG configuration, you cannot configure MAC limiting on the interchassis link (ICL) interface.

drop-and-log—(EX Series switches and QFX Series only) Drop packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

log—(EX Series switches and QFX Series only) Hold packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

none—(EX Series switches and QFX Series only) Forward packets with new source MAC addresses, and learn the new source MAC address.

shutdown—(EX Series switches and QFX Series only) Disable the specified interface, and generate an alarm, an SNMP trap, or a system log entry.

Required Privilege Level
 routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.

- Related Documentation**
- *Configuring EVPN Routing Instances*
 - *Configuring EVPN Routing Instances on EX9200 Switches*
 - *Configuring MAC Limiting (ELS)*
 - [Configuring Persistent MAC Learning \(ELS\) on page 337](#)
 - *Understanding Layer 2 Learning and Forwarding for Bridge Domains*
 - *Layer 2 Learning and Forwarding for VLANs Overview*
 - *Understanding Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports*
 - *Layer 2 Learning and Forwarding for VLANs Overview*
 - *Layer 2 Learning and Forwarding for VLANs Acting as a Switch for a Layer 2 Trunk Port*

path-length

Syntax	<code>path-length <i>certificate-path-length</i>;</code>
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificate path length.
Options	<i>certificate-path-length</i> —Digital certificate path length. Range: 2 through 15 certificates Default: 15 certificates
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Path Length for the Certificate Hierarchy on page 181

perfect-forward-secrecy (Security)

Syntax	<pre>perfect-forward-secrecy { keys (group1 group2); }</pre>
Hierarchy Level	[edit security ipsec policy <i>ipsec-policy-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the Perfect Forward Secrecy (PFS) protocol. Create single-use keys.
Options	<p>keys—Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange.</p> <p>The key can be one of the following:</p> <ul style="list-style-type: none">• group1—768-bit.• group2—1024-bit.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the IPsec Policy for an ES PIC on page 49

perfect-forward-secrecy (Services)

Syntax	<pre>perfect-forward-secrecy { keys (group1 group2 group5 group14 group15 group16 group24); }</pre>
Hierarchy Level	<code>[edit services ipsec-vpn ipsec policy <i>policy-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. group15 , group16 , and group24 options added in Junos OS Release 17.4R1.
Description	Define Perfect Forward Secrecy (PFS). Creates single-use keys. This statement is optional.
Options	keys —Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange. The key can be one of the following: group1 —768-bit. group2 —1024-bit. group5 —1536-bit. group14 —2048-bit. group15 —3072-bit. group16 —4096-bit. group24 —2048-bit with 256-bit Prime Order Subgroup.
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring IPsec Policies</i>


persistent-learning

Syntax	<code>persistent-learning;</code>
Hierarchy Level	<ul style="list-style-type: none"> For platforms without ELS: <code>[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)]</code> For platforms with ELS: <code>[edit switch-options <i>interface</i> <i>interface-name</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 11.4 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Hierarchy level <code>[edit switch-options interface interface-name]</code> introduced in Junos OS Release 13.2X50-D10</p>
Description	Specify that learned MAC addresses persist on the specified interfaces across restarts of the switch and link-down conditions. This feature is also known as sticky MAC.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system—control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Example: Configuring Port Security (non-ELS) on page 15 Configuring Persistent MAC Learning (non-ELS) on page 338 Configuring Persistent MAC Learning (ELS) on page 337

persistent-learning

Syntax	<code>persistent-learning;</code>
Hierarchy Level	[edit switch-options interface <i>interface-name</i>]
Release Information	Hierarchy level [edit switch-options interface interface-name] introduced in Junos OS Release 13.2X50-D10
Description	Specify that learned MAC addresses persist on the specified interfaces across restarts of the switch and link-down conditions. This feature is also known as sticky MAC.
Required Privilege Level	system—To view this statement in the configuration. system—control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Port Security (non-ELS) on page 15• Configuring Persistent MAC Learning (ELS) on page 337

physical-interface (DDoS Flow Detection)

Syntax	<code>physical-interface (flow-bandwidth flow-control-mode flow-detection-mode)</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers. Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure flow bandwidth, flow control mode, or flow detection mode at the physical interface flow aggregation level for the packet type.
Options	<p>flow-bandwidth—Bandwidth for the flow at the physical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth] hierarchy level.</p> <p>Default: 20,000 packets per second</p> <p>Range: 1 through 50,000 packets per second</p> <p>flow-control-mode—Mode for how traffic in the detected flow is controlled at the physical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control] hierarchy level.</p>
	<p> NOTE: The configuration at this level overrides the global configuration using the flow-level-control statement at the [edit system ddos-protection global] hierarchy level.</p>
	<ul style="list-style-type: none"> drop—Drop all traffic in flow. keep—Keep all traffic in flow. police—Police the traffic to within its allowed bandwidth. <p>Default: drop</p> <p>flow-detection-mode—Mode for how flow detection operates at the physical interface level when a policer has been violated. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection] hierarchy level.</p>



NOTE: The configuration at this level overrides the global configuration using the `flow-detection-mode` statement at the `[edit system ddos-protection global]` hierarchy level.

- **automatic**—Search flows at the physical interface level only when a DDoS policer is being violated and only when the policer violation is not discovered at the finer aggregation levels, logical interface or subscriber. Flows at the physical interface level are subsequently not searched again until a subsequent violation occurs that cannot be found at the subscriber or logical interface levels.
- **off**—Disable flow detection at the physical interface level so that flows are never searched at this level.
- **on**—Search flows at the physical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

Default: `automatic`

Required Privilege Level	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
---------------------------------	---

- | | |
|------------------------------|--|
| Related Documentation | <ul style="list-style-type: none">• Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 575• Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 572• Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 571• Configuring Flow Detection for DDoS Protection |
|------------------------------|--|

pki

```

Syntax  pki {
        auto-re-enrollment {
            certificate-id {
                ca-profile ca-profile-name;
                challenge-password password;
                re-enroll-trigger-time-percentage percentage;
                re-generate-keypair;
                validity-period days;
            }
        }
        ca-profile ca-profile-name {
            ca-identity ca-identity;
            enrollment {
                url url-name;
                retry number-of-enrollment-attempts;
                retry-interval seconds;
            }
            revocation-check {
                disable;
                crl {
                    disable on-download-failure;
                    refresh-interval hours;
                    url {
                        url-name;
                        password;
                    }
                }
            }
        }
        traceoptions {
            file filename <files number> <match regular-expression> <size maximum-file-size>
              <world-readable | no-world-readable>;
            flag flag;
        }
    }

```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 7.5.
revocation-check and **crl** statements added in Junos OS Release 8.1.

Description Configure an IPsec profile to request digital certificates for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M Series and T Series routers.

Options The remaining statements are explained separately.

Required Privilege admin—To view this statement in the configuration.
Level admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Digital Certificates for Adaptive Services Interfaces on page 185](#)
- [CLI Explorer](#)

policy

Syntax

```

policy policy-name {
  accept {
    match-list {
      match-criteria {
        (match-all | match-any);
      }
      prefix-list-name prefix-list-name;
      source-ip-address-list address-list-name;
      source-mac-address-list address-list-name;
    }
    match-option {
      hop-limit {
        (maximum | minimum) value;
      }
      managed-config-flag;
      other-config-flag;
      router-preference (high | low | medium);
    }
  }
  discard {
    prefix-list-name prefix-list-name;
    source-ip-address-list address-list-name;
    source-mac-address-list address-list-name;
  }
}

```

Hierarchy Level

```

[edit forwarding-options access-security router-advertisement-guard]
[edit forwarding-options access-security router-advertisement-guard interface
interface-name]
[edit forwarding-options access-security router-advertisement-guard vlans (vlan-name |
all)]

```

Release Information Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.
Statement introduced in Junos OS Release 16.1 for EX Series switches.

Description Configure the policy for an IPv6 Router Advertisement (RA) guard. RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages based on whether they match the conditions defined in the policy.

RA guard compares the information contained in attributes of RA messages to the information contained in the policy. You must configure the policy before you can enable RA guard. You can configure either an accept policy or a discard policy and enable it on an interface or on a VLAN. When RA guard is enabled by using an accept policy, any RA messages that match the conditions defined in the policy are forwarded, and RA messages that do not match the conditions are dropped. When RA guard is enabled by using a

discard policy, any RA messages that match the conditions defined in the policy are dropped, and RA messages that do not match the conditions are forwarded.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Stateless IPv6 Router Advertisement Guard on page 517](#)
- [Configuring Stateful IPv6 Router Advertisement Guard on page 514](#)

policy (Security IKE)

Syntax

```
policy ike-peer-address {  
  description policy-description;  
  encoding (binary | pem);  
  identity identity-name;  
  local-certificate certificate-filename;  
  local-key-pair private-public-key-file;  
  mode (aggressive | main);  
  pre-shared-key (ascii-text key | hexadecimal key);  
  proposals [ proposal-names ];  
}
```

Hierarchy Level [edit security [ike](#)]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define an IKE policy.

Options *ike-peer-address*—A tunnel address configured at the [\[edit interfaces es\]](#) hierarchy level.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.


Related Documentation

- [Configuring an IKE Policy for Preshared Keys on page 44](#)
- [Configuring an IKE Policy for Digital Certificates for an ES PIC on page 182](#)

policy (Security IPsec)

Syntax	<pre> policy <i>ipsec-policy-name</i> { description <i>description</i>; perfect-forward-secrecy { keys (group1 group 14 group2 group 5); } proposals [<i>proposal-names</i>]; } </pre>
Hierarchy Level	[edit security ipsec]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define an IPsec policy.
Options	<p><i>ipsec-policy-name</i>—Specify an IPsec policy name.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring the IPsec Policy for an ES PIC on page 49

port-error-disable

Syntax	<pre>port-error-disable { disable-timeout <i>timeout</i> ; }</pre>
Hierarchy Level	[edit ethernet-switching-options],
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches.
Description	<p>Disable rather than block an interface when enforcing MAC limiting, MAC move limiting, and rate-limiting configuration options for shutting down the interface, and allow the interface to recover automatically from the error condition after a specified period of time:</p> <ul style="list-style-type: none"> If you have enabled MAC limiting with the shutdown option and you enable port-error-disable, the switch disables (rather than shuts down) the interface when the MAC address limit is reached. If you have enabled MAC move limiting with the shutdown option and you enable port-error-disable, the switch disables (rather than shuts down) the interface when the maximum number of moves to a new interface is reached. If you have enabled storm control with the action-shutdown option and you enable port-error-disable, the switch disables (rather than shuts down) the interface when applicable traffic exceeds the specified levels. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> NOTE: The port-error-disable configuration does not apply to pre-existing error conditions. It impacts only error conditions that are detected after port-error-disable has been enabled and committed. To clear a pre-existing error condition and restore the interface to service, use the operational command that appears in your CLI:</p> <ul style="list-style-type: none"> clear ethernet-switching port-error </div> <p>The remaining statement is explained separately. See CLI Explorer.</p>
Default	Not enabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system—control—To add this statement to the configuration.</p>

- Related Documentation**
- [action-shutdown on page 667](#)
 - *Configuring MAC Move Limiting (non-ELS)*

port-id

Syntax	<code>port-id port-id-number;</code>
Hierarchy Level	[edit security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name id]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specify a port ID in a secure channel when enabling MACsec using static secure association key (SAK) security mode. The port IDs must match on a sending and receiving secure channel on each side of a link to enable MACsec.</p> <p>Once the port numbers match, MACsec is enabled for all traffic on the connection.</p> <p>You only use this configuration option when you are configuring MACsec using static SAK security mode. This option does not need to be specified when you are enabling MACsec using static connectivity association key (CAK) security mode.</p>
Default	No port ID is specified.
Options	<i>port-id-number</i> —The port ID number.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

port-id (MACsec for MX Series)

Syntax	<code>port-id <i>port-id-number</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> secure-channel <i>secure-channel-name</i> id]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specify a port ID in a secure channel when enabling MACsec using static secure association key (SAK) security mode. The port IDs must match on a sending and receiving secure channel on each side of a link to enable MACsec.</p> <p>Once the port numbers match, MACsec is enabled for all traffic on the connection.</p> <p>You only use this configuration option when you are configuring MACsec using static SAK security mode. This option does not need to be specified when you are enabling MACsec using static connectivity association key (CAK) security mode.</p>
Default	No port ID is specified.
Options	<i>port-id-number</i> —The port ID number.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

prefix (Circuit ID for Option 82)

Syntax

```
prefix {
  host-name;
  logical-system-name;
  routing-instance-name;
}
```

Hierarchy Level

- For platforms with enhanced Layer 2 software (ELS):

```
[edit vlans forwarding-options dhcp-security option-82 circuit-id]
```

- For platforms without ELS:

```
[edit ethernet-switching-options secure-access-port vlan (all | vlan-name) dhcp-option82
circuit-id],
[edit forwarding-options helpers bootp dhcp-option82 circuit-id],
[edit forwarding-options helpers bootp interface interface-name dhcp-option82 circuit-id]
```

- For MX Series platforms:

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security
option-82circuit-id]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level `[edit vlans vlan-name forwarding-options dhcp-security option-82 circuit-id]` introduced in Junos OS Release 13.2X50-D10. (See *Using the Enhanced Layer 2 Software CLI* for information about ELS.)
Statement introduced in Junos OS Release 14.1 for the MX Series.

Description

Configure an optional prefix for the circuit ID suboption in the DHCP option 82 information that is inserted by the switch or router into the packet header of a DHCP request before it forwards or relays the request to a DHCP server.

Default

If the **prefix** statement is not explicitly specified, no prefix is prepended to the circuit ID.

Options

host-name—Add router host name to DHCP option 82 circuit ID.

logical-system-name—Add logical system name to DHCP option-82 circuit ID.

This option is not used for the **prefix** statement at any of the above hierarchy levels.

routing-instance-name—Add routing instance name to DHCP option-82 circuit ID.

This option is not used for the **prefix** statement occurring at the following hierarchy levels:

- [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82 *circuit-id*]
- Any of the hierarchy levels for the platforms without ELS

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

- Related Documentation**
- [Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443](#)
 - [Example: Setting Up DHCP Option 82 on page 433](#)
 - RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.

prefix (DHCPv6 Options)

Syntax	<pre> prefix { host-name; logical-system-name; routing-instance-name; vlan-id; vlan-name; } </pre>
Hierarchy Level	[edit vlans forwarding-options dhcp-security dhcpv6-options option-18] [edit vlans forwarding-options dhcp-security dhcpv6-options option-37]
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Configure a prefix for DHCPv6 option 18 (Interface ID) or option 37 (Remote ID). When configured, the prefix is inserted into DHCPv6 packets during the DHCPv6 snooping process.
Default	If the prefix statement is not explicitly specified, no prefix is inserted in DHCPv6 packets.
Options	<p>host-name—Add the host name of the switch to DHCPv6 options.</p> <p>logical-system-name—Add the logical system name to the DHCPv6 options.</p> <p>routing-instance-name—Add the routing instance name to the DHCPv6 options.</p> <p>vlan-id—Add the VLAN ID to the DHCPv6 options.</p> <p>vlan-name—Add the VLAN name to the DHCPv6 options.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • option-37 (DHCPv6 Snooping) on page 901 • option-18 (DHCPv6 Snooping) on page 899

prefix (Remote ID for Option 82)

Syntax	prefix (hostname mac none);
Hierarchy Level	<pre>[edit ethernet-switching-options secure-access-port vlan (all vlan-name) dhcp-option82 remote-id]</pre> <pre>[edit forwarding-options helpers bootp dhcp-option82 remote-id]</pre> <pre>[edit forwarding-options helpers bootp interface interface-name dhcp-option82 remote-id]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p>
Description	Configure an optional prefix for the remote ID suboption in the DHCP option 82 information that is inserted by the switch into the packet header of a DHCP request before it forwards or relays the request to a DHCP server.
Default	If prefix is not explicitly specified, no prefix is appended to the remote ID.
Options	<p>hostname—Name of the host system (the switch) that is forwarding or relaying the DHCP request from the DHCP client to the DHCP server.</p> <p>mac—MAC address of the host system (the switch) that is forwarding or relaying the DHCP request from the DHCP client to the DHCP server.</p> <p>none—No prefix is applied to the remote ID.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443 • Example: Setting Up DHCP Option 82 on page 433 • RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046.

prefix-list-name

Syntax	<code>prefix-list-name <i>prefix-list-name</i>;</code>
Hierarchy Level	<p>[edit forwarding-options access-security router-advertisement-guard policy <i>policy-name</i> discard]</p> <p>[edit forwarding-options access-security router-advertisement-guard policy <i>policy-name</i> accept match-list]</p>
Release Information	<p>Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.</p> <p>Statement introduced in Junos OS Release 16.1 for EX Series switches.</p>
Description	<p>Configure a list of IPv6 address prefixes for an IPv6 Router Advertisement (RA) guard policy. The policy is used to validate the source IPv6 address prefix of an incoming RA message against the IPv6 address prefixes in this list. RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in the policy.</p> <p>You can use a list of IPv6 address prefixes for validating RA messages as part of either an accept policy or a discard policy. Before you can include a list in an RA guard policy, you must configure the list name at the [edit policy-options prefix-list] hierarchy level. When RA guard is enabled by using an accept policy, any RA messages that match the conditions defined in the policy are forwarded, and RA messages that do not match the conditions are dropped. When RA guard is enabled by using a discard policy, any RA messages that match the conditions are dropped, and RA messages that do not match the conditions are forwarded.</p>
Options	<p><i>prefix-list-name</i>—Configure a list of IPv6 address prefixes for an RA guard policy. The policy is used to validate the source of an incoming RA message by comparing the IPv6 address prefix of the RA message to the IPv6 address prefixes contained in the list.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514

pre-shared-key

Syntax	<pre>pre-shared-key { cak hexadecimal-number; ckn hexadecimal-number; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specifies the pre-shared key used to enable MACsec using static connectivity association key (CAK) security mode.</p> <p>A pre-shared key includes a connectivity association key name (CKN) and a connectivity association key (CAK). A pre-shared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using static CAK security mode. The MACsec Key Agreement (MKA) protocol is enabled after the pre-shared keys are successfully verified and exchanged. The pre-shared key—the CKN and CAK—must match on both ends of a link.</p>
Default	No pre-shared keys exist, by default.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228

pre-shared-key (MX Series)

Syntax	<pre>pre-shared-key { cak hexadecimal-number; ckn hexadecimal-number; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specifies the pre-shared key used to enable MACsec using static connectivity association key (CAK) security mode.</p> <p>A pre-shared key includes a connectivity association key name (CKN) and a connectivity association key (CAK). A pre-shared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using static CAK security mode. The MACsec Key Agreement (MKA) protocol is enabled after the pre-shared keys are successfully verified and exchanged. The pre-shared key—the CKN and CAK—must match on both ends of a link.</p>
Default	No pre-shared keys exist, by default.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

pre-shared-key (Security)

Syntax	pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the key used to authenticate a dynamic peer during IKE phase 1 negotiation. Specify the key in either ASCII or hexadecimal format.
Options	ascii-text <i>key</i> —Authentication key in ASCII format. hexadecimal <i>key</i> —Authentication key in hexadecimal format.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an IKE Policy for Preshared Keys on page 44

priority (DDoS)

Syntax	<code>priority <i>level</i>;</code>
Hierarchy Level	<ul style="list-style-type: none"> For MX Series routers, T4000 routers, and EX9200 switches: <code>[edit system ddos-protection protocols <i>protocol-group packet-type</i>]</code> For PTX Series routers and QFX Series switches: <code>[edit system ddos-protection protocols <i>protocol-group packet-type</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.</p> <p>Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.</p>
Description	(MX Series routers with only MPCs, T4000 routers with only FPC5s, PTX Series routers, EX9200 switches, or QFX Series switches) Configure the priority for the packet type within the parent protocol group. In the event of downstream traffic congestion, high priority packets are provided bandwidth before medium priority packets. In turn, medium priority packets are provided bandwidth before low priority packets. Packets are dropped when there is insufficient available bandwidth.
Options	<i>level</i> —Priority of the packet type, low, medium, or high.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537

proposal (Security IKE)

Syntax `proposal ike-proposal-name {
 authentication-algorithm (md5 | sha1 | sha-256);
 authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
 description description;
 dh-group (group1 | group2 | group 5 | group14);
 encryption-algorithm algorithm;
 lifetime-seconds seconds;
 }`

Hierarchy Level `[edit security ike]`

Release Information Statement introduced before Junos OS Release 7.4.

Description Define an IKE proposal for a dynamic SA.

Options *ike-proposal-name*—Specify an IKE proposal name.

 The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.

Related Documentation • *Configuring an IKE Proposal for Dynamic SAs*

proposal (Security IPsec)

Syntax	<pre>proposal <i>ipsec-proposal-name</i> { authentication-algorithm (hmac-md5-96 hmac-sha1-96); encryption-algorithm <i>algorithm</i>; lifetime-seconds <i>seconds</i>; protocol (ah bundle esp); }</pre>
Hierarchy Level	[edit security ipsec]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define an IPsec proposal for a dynamic SA.
Options	<p><i>ipsec-proposal-name</i>—Specify an IPsec proposal name.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an IPsec Proposal for an ES PIC on page 47

proposals

Syntax	<code>proposals [<i>proposal-names</i>];</code>
Hierarchy Level	<code>[edit security ike policy <i>ike-peer-address</i>],</code> <code>[edit security ipsec policy <i>ipsec-policy-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Associate one or more proposals with an IKE or IPsec policy.
Options	<i>proposal-names</i> —Name of one or more proposals.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an IKE Policy for Preshared Keys on page 44• Configuring the IPsec Policy for an ES PIC on page 49

protocol (Junos OS)

Syntax	<code>protocol (ah esp bundle);</code>
Hierarchy Level	<code>[edit security ipsec proposal <i>ipsec-proposal-name</i>],</code> <code>[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound </code> <code>bidirectional)]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the IPsec protocol for a manual or dynamic SA.



NOTE: The Junos OS supports only encapsulating security payload (ESP) when you use tunnel mode.

In transport mode, the Junos OS does not support authentication header (AH) and ESP header bundles.

In transport mode, the Junos OS supports only Border Gateway Protocol (BGP).

Options	<p>ah—Authentication Header protocol</p> <p>bundle—AH and ESP protocols</p> <p>esp—ESP protocol (the tunnel statement must be included at the <code>[edit security ipsec security-association <i>sa-name</i> mode</code> hierarchy level)</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Using IPsec to Protect BGP Traffic • Configuring Manual IPsec Security Associations for an ES PIC on page 39 • Configuring the Protocol for a Dynamic IPsec SA on page 49

protocol (Junos-FIPS Software)

Syntax	protocol esp;
Hierarchy Level	[edit security ipsec internal security-association manual direction]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	The protocol used for the internal Routing-Engine-to-Routing-Engine IPsec security association (SA) configuration.
Options	Only esp is supported.
Required Privilege Level	Crypto Officer—To add and view this statement in the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 211• <i>Secure Configuration Guide for Common Criteria and Junos-FIPS</i>

protocols (DDoS)

Syntax

```
protocols protocol-group (aggregate | packet-type) {
    bandwidth packets-per-second;
    burst size;
    bypass-aggregate;
    disable-fpc;
    disable-logging;
    disable-routing-engine;
    flow-detection-mode (automatic | off | on);
    flow-detect-time seconds;
    flow-level-bandwidth {
        logical-interface flow-bandwidth;
        physical-interface flow-bandwidth;
        subscriber flow-bandwidth;
    }
    flow-level-control {
        logical-interface flow-control-mode;
        physical-interface flow-control-mode;
        subscriber flow-control-mode;
    }
    flow-level-detection {
        logical-interface flow-operation-mode;
        physical-interface flow-operation-mode;
        subscriber flow-operation-mode;
    }
    flow-recover-time seconds;
    flow-timeout-time seconds;
    fpc slot-number {
        bandwidth-scale percentage;
        burst-scale percentage;
        disable-fpc;
    }
    no-flow-logging
    priority level;
    recover-time seconds;
    timeout-active-flows;
}
```

Hierarchy Level [edit system [ddos-protection](#)]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure DDoS policers for all packet types within a protocol group or for a particular packet type within a protocol group.

Options **aggregate**—Configure the policer to monitor all control packets within the protocol group. You can configure an aggregate policer for any protocol group.

packet-type—(Optional) Name of the control packet type to be policed. You can configure a specific policer for only the following packet types and protocol groups:

- **arp**—The following ARP packet types are available:
 - **aggregate**—Applies to the combination of all types of control packet traffic for this protocol group.
- **bgp**—The following BGP packet types are available:
 - **aggregate**—Applies to the combination of all types of control packet traffic for this protocol group.
- **bgpv6**—The following BGPv6 packet types are available:
 - **aggregate**—Applies to the combination of all types of control packet traffic for this protocol group.
- **dhcpv4**—The following packet types are available for DHCPv4 traffic:
 - **ack**—DHCPACK packets.
 - **bad-packets**—DHCPv4 packets with bad formats.
 - **bootp**—DHCPBOOTP packets.
 - **decline**—DHCPDECLINE packets.
 - **discover**—DHCPDISCOVER packets.
 - **force-renew**—DHCPFORCERENEW packets.
 - **inform**—DHCPINFORM packets.
 - **lease-active**—DHCPLEASEACTIVE packets.
 - **lease-query**—DHCPLEASEQUERY packets.
 - **lease-unassigned**—DHCPLEASEUNASSIGNED packets.
 - **lease-unknown**—DHCPLEASEUNKNOWN packets.
 - **nak**—DHCPNAK packets.
 - **no-message-type**—DHCP packets that are missing the message type.
 - **offer**—DHCPOFFER packets.
 - **release**—DHCPRELEASE packets.
 - **renew**—DHCPRENEW packets.
 - **request**—DHCPREQUEST packets.
 - **unclassified**—All unclassified packets in the protocol group.
- **dhcpv6**—The following packet types are available for DHCPv6 traffic:

- **advertise**—ADVERTISE packets.
- **confirm**—CONFIRM packets.
- **decline**—DECLINE packets.
- **information-request**—INFORMATION-REQUEST packets.
- **leasequery**—LEASEQUERY packets.
- **leasequery-data**—LEASEQUERY-DATA packets.
- **leasequery-done**—LEASEQUERY-DONE packets.
- **leasequery-reply**—LEASEQUERY-REPLY packets.
- **rebind**—REBIND packets.
- **reconfigure**—RECONFIGURE packets.
- **relay-forward**—RELAY-FORWARD packets.
- **relay-reply**—RELAY-REPLY packets.
- **release**—RELEASE packets.
- **renew**—RENEW packets.
- **reply**—REPLY packets.
- **request**—REQUEST packets.
- **solicit**—SOLICIT packets.
- **unclassified**—All unclassified packets in the protocol group.
- **filter-action**—The following packet types are available for unclassified firewall filter action packets, sent to the host because of reject terms in firewall filters:
 - **filter-v4**—Unclassified IPv4 filter action packets.
 - **filter-v6**—Unclassified IPv6 filter action packets.
 - **other**—All other unclassified filter action packets that are not IPv4 or IPv6.
- **frame-relay**—The following packet types are available for Frame Relay traffic:
 - **frf15**—Multilink frame relay FRF.15 packets.
 - **frf16**—Multilink frame relay FRF.16 packets.
- **ip-fragments**—The following packet types are available for IP fragments:
 - **first-fragment**—First IP fragment.
 - **trail-fragment**—Last IP fragment.

- **ip-options**—The following packet types are available for IP option traffic:
 - **non-v4v6**—Options packets other than IPv4/v6.
 - **router-alert**—Router alert options packets.
 - **unclassified**—All unclassified packets in the protocol group.
- **l2tp**—The following packet types are available for L2TP traffic:
 - **cdn**—Call-Disconnect-Notify message packets.
 - **hello**—Hello message packets.
 - **iccn**—Incoming-Call-Connected message packets.
 - **icrq**—Incoming-Call-Request message packets.
 - **scccn**—Start-Control-Connection-Connected message packets.
 - **sccrq**—Start-Control-Connection-Request message packets.
 - **stopccn**—Stop-Control-Connection-Notification message packets.
 - **unclassified**—All unclassified packets in the protocol group.
- **mcast-snoop**—Control traffic for multicast snooping.
 - **igmp**—Snooped IGMP traffic.
 - **mld**—Snooped MLD traffic.
 - **pim**—Snooped PIM control traffic.
- **mlp**—The following MLP packet types are available:
 - **aggregate**—Applies to the combination of all types of control packet traffic for this protocol group.
 - **add**—Add requests; internal MAC address learning request packets sent to the host.
 - **delete**—Delete requests; internal MAC address learning request packets sent to the host.
 - **lookup**—Lookup requests; internal MAC address learning request packets sent to the host.
 - **unclassified**—All unclassified packets in the protocol group.
 - **macpin-exception**—Exceptions to MAC address pinning (wherein dynamically learned MAC addresses are pinned to prevent looping caused by MAC moves from duplicate MAC detection).

- **ndpv6**—The following NDPv6 packet types are available, except where noted, starting in 14.1R8, 14.2R8, 15.1R5, 15.1F7, and 16.1R1:
 - **aggregate**—Applies to the combination of all types of control packet traffic for this protocol group.
 - **invalid-hop-limit**—(Starting in 16.1R2) Invalid hop limit packets. These messages might represent crafted packets in a malicious network-based packet flood.
 - **neighbor-advertisement**—Neighbor advertisement packets. These are messages used for duplicate address detection and to test reachability of neighbors. Neighbor advertisements are sent in response to neighbor solicitation messages.
 - **neighbor-solicitation**—Neighbor solicitation packets. These are messages used for duplicate address detection and to test reachability of neighbors.
 - **redirect**—Redirect packets.
 - **router-advertisement**—Router advertisement packets. These are messages sent to announce the presence of the router, advertise prefixes, assist in address configuration, and share other link information such as MTU size and hop limit. The IPv6 nodes on the link can use this information to configure themselves with an IPv6 address and routing information such as the default gateway.
 - **router-solicitation**—Router solicitation packets. These are messages sent by IPv6 nodes when they come online to solicit immediate router advertisements from the router.
- **ppp**—The following PPP packet types are available:
 - **authentication**—PPP authentication protocol packets.
 - **echo-rep**—LCP echo reply packets.
 - **echo-req**—LCP echo request packets.
 - **ipcp**—IP Control Protocol packets.
 - **ipv6cp**—IPv6 Control Protocol packets.
 - **isis**—IS-IS packets.
 - **lcp**—Link Control Protocol packets.
 - **mlppp-lcp**—MLPPP LCP packets.
 - **mplscp**—MPLS Control Protocol packets.
 - **unclassified**—All unclassified packets in the protocol group.

- **pppoe**—The following PPPoE packet types are available:
 - **padi**—PADI packets.
 - **padm**—PADM packets.
 - **padn**—PADN packets.
 - **pado**—PADO packets.
 - **padr**—PADR packets.
 - **pads**—PADS packets.
 - **padt**—PADT packets.
- **radius**—The following RADIUS packet types are available:
 - **accounting**—RADIUS accounting packets.
 - **authorization**—RADIUS authorization packets.
 - **server**—RADIUS server traffic.
 - **unclassified**—All unclassified packets in the protocol group.
- **re-services**—The following packet type is available for Routing Engine-based HTTP redirect IPv4 traffic:
 - **captive-portal**—Routing Engine-based captive portal content delivery packets.
- **re-services-v6**—The following packet type is available for Routing Engine-based HTTP redirect IPv6 traffic:
 - **captive-portal**—Routing Engine-based captive portal content delivery packets.
- **resolve**—The following packet types are available for unclassified resolve packets, which are sent to the host because of a traffic request resolve action:
 - **mcast-v4**—Unclassified IPv4 multicast resolve packets.
 - **mcast-v6**—Unclassified IPv6 multicast resolve packets.
 - **ucast-v4**—Unclassified IPv4 unicast resolve packets.
 - **ucast-v6**—Unclassified IPv6 unicast resolve packets.
 - **other**—All other unclassified resolve packets.
- **sample**—The following sample packet types are available:
 - **host**—Host packets.
 - **pfe**—Packet Forwarding Engine packets.
 - **syslog**—System log message packets.
 - **tap**—TAP packets.

- **tcp-flags**—The following TCP-flagged packet types are available:
 - **established**—TCP packets with ACK or RST flags set.
 - **initial**—TCP packets with SYN flag set and ACK flag not set.
 - **unclassified**—TCP packets with flags set any other way than the established and initial packets.
- **unclassified**—The following unclassified packet types are available:
 - **control-layer2**—Unclassified layer 2 control packets.
 - **control-v4**—Unclassified IPv4 control packets.
 - **control-v6**—Unclassified IPv6 control packets.
 - **fw-host**—Unclassified send-to-host firewall packets.
 - **host-route-v4**—Unclassified IPv4 routing protocol and host packets in traffic sent to the router local interface address.
 - **host-route-v6**—Unclassified IPv6 routing protocol and host packets in traffic sent to the router local interface address.
 - **other**—All unclassified packets that do not belong to another type.
- **virtual-chassis**—The following packet types are available for virtual chassis packets:
 - **control-low**—Low-priority control packets.
 - **control-high**—High-priority control packets.
 - **unclassified**—All unclassified packets in the protocol group.
 - **vc-packets**—All exception packets on the virtual chassis link.
 - **vc-ttl-errors**—Virtual chassis TTL error packets.

protocol-group—Name of the protocol group for which traffic is policed. You can configure a policer for any of the following protocol groups:

- **amtv4**—IPv4 AMT traffic.
- **amtv6**—IPv6 AMT traffic.
- **ancp**—ANCP traffic.
- **ancpv6**—ANCPv6 traffic.
- **arp**—ARP traffic.
- **atm**—ATM traffic.
- **bfd**—BFD traffic.
- **bfdv6**—BFDv6 traffic.
- **bgp**—BGP traffic.
- **bgpv6**—BGPv6 traffic.
- **control**—Control traffic.
- **demux-autosense**—Demux autosensing traffic.
- **dhcipv4**—DHCPv4 traffic.
- **dhcipv6**—DHCPv6 traffic.
- **diameter**—Diameter and Gx-Plus traffic.
- **dns**—DNS traffic.
- **dtcp**—DTCP traffic.
- **dynamic-vlan**—Dynamic VLAN exception traffic.
- **egpv6**—EGPv6 traffic.
- **eoam**—EOAM traffic.
- **esmc**—ESMC traffic.
- **fab-probe**—Fab out probe packets.
- **filter-action**—IPv4 and IPv6 firewall filter action packets sent to the host because of reject terms in firewall filters
- **frame-relay**—Frame relay traffic.
- **ftp**—FTP traffic.
- **ftpv6**—FTPv6 traffic.
- **gre**—GRE traffic.
- **icmp**—ICMP traffic.
- **igmp**—IGMP traffic
- **igmpv4v6**—IGMP v4/v6 traffic.

- **igmpv6**—IGMPv6 traffic.
- **inline-ka**—Inline service interfaces keepalive traffic.
- **inline-svcs**—Inline services traffic.
- **ip-fragments**—IP fragments traffic.
- **ip-options**—IP traffic with IP packet header options.
- **isis**—IS-IS traffic.
- **jfm**—JFM traffic.
- **l2pt**—Layer 2 protocol tunneling traffic.
- **lACP**—LACP traffic.
- **ldp**—LDP traffic.
- **ldpv6**—LDPv6 traffic.
- **lldp**—LLDP traffic.
- **lmp**—LMP traffic.
- **lmpv6**—LMPv6 traffic.
- **mac-host**—Layer 2 MAC send-to-host traffic.
- **mcast-snoop**—Control traffic for multicast snooping.
- **mlp**—MLP traffic.
- **msdp**—MSDP traffic.
- **msdpv6**—MSDPv6 traffic.
- **multicast-copy**—Host copy traffic due to multicast routing.
- **mvrp**—MVRP traffic.
- **ndpv6**—NDPv6 traffic.
- **ntp**—NTP traffic.
- **oam-lfm**—OAM-LFM traffic.
- **ospf**—OSPF traffic.
- **ospfv3v6**—OSPFv3/IPv6 traffic.
- **pfe-alive**—Packet Forwarding Engine keepalive traffic.
- **pim**—PIM traffic.
- **pimv6**—PIMv6 traffic.
- **pmvrp**—PMVRP traffic.
- **pos**—POS traffic.
- **ppp**—PPP traffic.

- **pppoe**—PPPoE traffic.
- **ptp**—PTP traffic.
- **pvstp**—PVSTP traffic.
- **radius**—RADIUS traffic.
- **re-services**—Captive portal content delivery IPv4 traffic for Routing Engine HTTP redirect.
- **re-services-v6**—Captive portal content delivery IPv6 traffic for Routing Engine HTTP redirect.
- **redirect**—Traffic that triggers ICMP redirects.
- **reject**—Packets rejected by a next-hop forwarding decision.
- **rejectv6**—V6 packets rejected by a next-hop forwarding decision.
- **resolve**—Unclassified IPv4 and IPv6 resolve packets sent to the host because of a traffic request resolve action.
- **rip**—RIP traffic.
- **ripv6**—RIPv6 traffic.
- **rsvp**—RSVP traffic.
- **rsvpv6**—RSVPv6 traffic.
- **services**—Service traffic.
- **snmp**—SNMP traffic.
- **snmpv6**—SNMPv6 traffic.
- **ssh**—SSH traffic.
- **sshv6**—SSHv6 traffic.
- **stp**—STP traffic.
- **syslog**—System log messages UDP traffic on port 6333 for the Routing Engine syslog server.
- **tacacs**—TACACS traffic.
- **tcp-flags**—Traffic with TCP flags.
- **telnet**—TELNET traffic.
- **telnetv6**—TELNETv6 traffic.
- **ttl**—TTL traffic.
- **tunnel-fragment**—Tunnel fragments traffic.
- **tunnel-ka**—Tunnel keepalive traffic.
- **unclassified**—Unclassified traffic.
- **virtual-chassis**—Virtual chassis traffic.

- **vrp**—VRRP traffic.
- **vrpv6**—VRRPv6 traffic.

The remaining statements are explained separately. Search for a statement in [CLI Explorer](#) or click a linked statement in the Syntax section for details.

Required Privilege	admin—To view this statement in the configuration.
Level	admin-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537• <i>Understanding Distributed Denial-of-Service Protection with IPv6 Neighbor Discovery Protocol</i>
------------------------------	--

protocols (DDoS) (PTX Series and QFX Series)

Syntax

```
protocols protocol-group (aggregate | packet-type) {
    bandwidth packets-per-second;
    burst size;
    bypass-aggregate;
    disable-fpc;
    disable-logging;
    fpc slot-number {
        bandwidth-scale percentage;
        burst-scale percentage;
        disable-fpc;
    }
    priority level;
}
```

Hierarchy Level [edit system [ddos-protection](#)]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.
Statement introduced in Junos OS Release 17.4R1 on PTX Series routers.

Description Configure DDoS policers for all packet types within a protocol group or for a particular packet type within a protocol group.



NOTE: PTX Series routers and QFX10002-60C switches do not support the `bypass-aggregate` option.

Not all protocol groups and packet types listed in [Table 36 on page 952](#) or [Table 37 on page 954](#) below are supported on all devices. Exceptions include:

- PTX Series routers do not support the following DDoS policer protocol group options: `all-fiber-channel-enode`, `arp-snoop`, `bridge-control`, `dhcpv4v6`, `diameter`, `garp-reply`, `martian-address`, `proto-802-1x`, `ptp`, `pvstp`, `radius`, `stp`, and `tacacs`
- QFX10002-60C switches do not support the following DDoS policer protocol group options: `all-fiber-channel-enode`, `arp-snoop`, `bridge-control`, `dhcpv4v6`, `diameter`, `garp-reply`, `martian-address`, `proto-802-1x`, `ptp`, `radius`, and `tacacs`

Options `aggregate`—Configure the policer that polices all control packets belonging to the specified protocol as a combined group. An aggregate policer exists for all protocol groups.

`packet-type`—Name of the control packet type to be policed.

On some devices, you can configure packet-type policers for the protocol groups listed in [Table 36 on page 952](#). For all other protocol groups not listed in [Table 36 on page 952](#), only aggregate policers are available.

[Table 36 on page 952](#) lists the protocol groups with packet-type policers available on some devices, and their default-configured parameters. Each of these protocol groups also support the aggregate policer. (See [Table 37 on page 954](#) for the default aggregate policer parameters for these protocol groups.)

Table 36: Packet Types Supported by DDoS Protection on PTX Series routers and QFX Series Switches

Protocol Group	Packet Type	Description	Default Bandwidth	Default Burst	Default Priority
arp	arp-snoop	ARP snooping traffic	500	2048	High
	unclassified	Unclassified ARP packets	500	1024	High
bfd	multihop-bfd	Multihop BFD traffic	1500	2048	High
	unclassified	Unclassified BFD packets	1000	2048	High
eoam	oam-cfm	Ethernet OAM CFM traffic	200	2048	High
	unclassified	Unclassified Ethernet OAM traffic	100000	2048	High
igmpv6	mld	MLD traffic	1000	2048	High
	unclassified	Unclassified IGMPv6 packets	90000	2048	High
mcast-snoop	igmp	Control packets for IGMP snooping	500	2048	High
	mld	Control packets for MLD snooping	500	2048	High
	pim	Control packets for PIM snooping	500	2048	High
	unclassified	Unclassified multicast snooping control packets	500	2048	High
radius	accounting	RADIUS accounting packets	200	2048	High
	authorization	RADIUS authorization packets	200	2048	High
	server	RADIUS server traffic	200	2048	High
	unclassified	Unclassified RADIUS traffic	200	2048	High
tcc	ethernet-tcc	TCC-encapsulated Ethernet traffic	100	2048	High
	iso-tcc	TCC-encapsulated ISO traffic	100	2048	High
	unclassified	Unclassified TCC-encapsulated traffic	100	2048	High

protocol-group—Name of the protocol group for which traffic is policed. You can configure the aggregate policer for any of the following protocol groups listed in [Table 37 on page 954](#). The table shows the aggregate policer default-configured parameters for each protocol group. Some protocol groups listed in the table can also have individual packet-type policers, which are listed in [Table 37 on page 954](#).

Table 37: Protocol Groups Supported by DDoS Protection on QFX Switches

Protocol Group	Description	Default Bandwidth	Default Burst
all-fiber-channel-enode	Fiber channel ENode traffic	10	2048
arp	ARP traffic	500	1024
arp-snoop	ARP snooping traffic NOTE: The arp protocol group option encompasses this as a packet type on some devices.	500	2048
bfd	Single-hop BFD traffic	1000	2048
bfdv6	BFDv6 traffic	3000	10000
bgp	BGP traffic	1500	2048
bridge-control	Bridge Control traffic	10	2048
dhcpv4v6	DHCPv4 and DHCPv6 traffic (limits apply to combined traffic)	500	2048
diameter	Diameter and Gx-Plus traffic	200	2048
dns	DNS traffic	200	2048
dtcp	DTCP traffic	200	2048
egpv6	EGPv6 traffic	10	2048
eoam	Ethernet OAM traffic	100000	2048
ethernet-tcc	TCC-encapsulated Ethernet traffic NOTE: The tcc protocol group option encompasses this as a packet type some devices.	100	2048
ftp	FTP traffic	500	2048
garp-reply	Gratuitous ARP reply traffic	100	2048
gre	GRE traffic	500	2048
icmp	ICMP traffic	500	2048

Table 37: Protocol Groups Supported by DDoS Protection on QFX Switches (continued)

Protocol Group	Description	Default Bandwidth	Default Burst
igmp	IGMPv4 and IGMPv6 traffic NOTE: Use this option on PTX Series and QFX10002-60C devices for IGMPv4 traffic only, and igmpv6 option for IGMPv6 traffic.	1000	2048
igmpv6	IGMPv6 traffic	90000	2048
ip-options	IP traffic with IP packet header options	100	2048
isis	IS-IS traffic	1000	2048
iso-tcc	TCC-encapsulated ISO traffic NOTE: The tcc protocol group option encompasses this as a packet type on some devices.	100	2048
l2pt	Layer 2 protocol tunneling traffic	500	2048
l2tp	Layer 2 tunneling protocol traffic	500	2048
lACP	LACP traffic	300	2048
ldp	LDP traffic	1000	200
ldp-hello	LDP hello packets	1000	2048
lldp	LLDP traffic	60	2048
lmp	LMP traffic	100	2048
martian-address	Martian address	200	20
mcast-snoop	Control traffic for multicast snooping	500	2048
mld	MLD traffic NOTE: The igmpv6 protocol group option encompasses this as a packet type on some devices.	1000	2048

Table 37: Protocol Groups Supported by DDoS Protection on QFX Switches (continued)

Protocol Group	Description	Default Bandwidth	Default Burst
msdp	MSDP traffic	300	2048
multihop-bfd	Multihop BFD traffic <i>NOTE:</i> The bfd protocol group option encompasses this as a packet type on some devices.	1500	2048
ndpv6	NDPv6 traffic	500	1024
ntp	NTP traffic	200	2048
oam-cfm	OAM CFM traffic <i>NOTE:</i> The eoam protocol group option encompasses this as a packet type on some devices.	200	2048
oam-lfm	OAM LFM traffic	200	2048
ospf	OSPF traffic	1000	200
ospf-hello	OSPF hello packets	1500	2048
pim-ctrl	PIM control packets	1000	2048
pim-data	PIM data	2000	2048
proto-802-lx	802.1X traffic	200	2048
ptp	PTP traffic	100	2048
pvstp	PVSTP traffic	2000	2048
radius	RADIUS traffic	200	2048
reject	Packets rejected by a next-hop forwarding decision	100	2048
resolve	Unclassified IPv4 and IPv6 resolve packets sent to the host because of a traffic request resolve action	500	2048
rip	RIP traffic	100	2048
rsvp	RSVP traffic	1000	2048

Table 37: Protocol Groups Supported by DDoS Protection on QFX Switches (continued)

Protocol Group	Description	Default Bandwidth	Default Burst
snmp	SNMP traffic	500	2048
ssh	SSH traffic	500	2048
stp	STP traffic	2000	2048
tacacs	TACACS+ traffic	200	2048
tcc	Transitional Cross-connect encapsulated traffic	100	2048
telnet	Telnet traffic	500	2048
tll	Time to Live packets	100	2048
unclassified	Traffic that cannot be classified into one of the other available protocol groups	100	2048
vrrp	VRRP traffic	1000	2048

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring DDoS Protection on page 535](#)

recover-time (DDoS)

Syntax	<code>recover-time <i>seconds</i>;</code>
Hierarchy Level	<code>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]</code>
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure how much time must pass since the last detected DDoS violation before the traffic is considered to have recovered from the attack and returned to normal.
Options	<i>seconds</i> —Period required for the traffic to recover. Range: 1 through 3600 seconds Default: 300
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DDoS Protection Aggregate or Individual Packet Type Policers on page 537

recovery-timeout

Syntax	<code>recovery-timeout <i>seconds</i>;</code>
Hierarchy Level (EX Series and QFX Series)	<code>[edit interfaces <i>interface-name</i> unit 0 family ethernet-switching]</code>
Hierarchy Level (MX Series)	<code>[edit interfaces <i>interface-name</i> unit 0 family bridge]</code>
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX Series. Statement introduced in Junos OS Release 14.1 for the MX Series routers.
Description	<p>Configure an interface to be temporarily disabled when MAC limiting, MAC move limiting, or rate-limiting is in effect with the action shutdown. This enables the affected interface to recover automatically from the error condition after the specified period of time:</p> <ul style="list-style-type: none"> • If you configure MAC limiting with the shutdown option and you enable recovery-timeout, the interface is temporarily disabled when the MAC address limit is reached. The interface will recover automatically after the number of seconds specified. • If you enable MAC move limiting with the shutdown option and you enable recovery-timeout, the interface is temporarily disabled when the maximum number of MAC address moves is reached. The interface will recover automatically after the number of seconds specified. • If you enable MAC move limiting with the vlan-member-shutdown option and you enable recovery-timeout, the interface is temporarily disabled when the maximum number of MAC address moves is reached. The interface will recover automatically after the number of seconds specified. If the recovery timeout is not configured, the interface will recover automatically after 180 seconds. • If you enable storm control with the action-shutdown option and you enable recovery-timeout, the interface is temporarily disabled when applicable traffic exceeds the specified levels. Depending upon the configuration, applicable traffic can include broadcast, unknown unicast, and multicast traffic.



NOTE: The **recovery-timeout** configuration does not apply to preexisting error conditions. It impacts only error conditions that are detected after the **recovery-timeout** statement is configured and committed. To clear a preexisting error condition and restore the interface to service, use the operational mode commands [clear ethernet-switching recovery-timeout](#) for EX Series and QFX Series and [clear bridge recovery-timeout](#) for MX Series routers.

Default The interface does not automatically recover from an error condition.



NOTE: On EX9200 switches, if a MAC move limit is configured with the action `vlan-member-shutdown`, the interface automatically recovers from the disabled condition after 180 seconds by default.

Options **seconds**— Number of seconds that the interface remains in a disabled state due to a port error prior to automatic recovery.
Range: 10 through 3600

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- [action-shutdown on page 667](#)
- [Configuring MAC Limiting \(ELS\)](#)
- [Configuring MAC Move Limiting \(ELS\) on page 365](#)
- [Enabling and Disabling Storm Control \(ELS\) on page 630](#)

re-enroll-trigger-time-percentage

Syntax re-enroll-trigger-time-percentage *percentage*;

Hierarchy Level [edit security [pki auto-re-enrollment certificate-id](#)]

Release Information Statement introduced in Junos OS Release 8.5.

Description Percentage of the router certificate [validity-period](#) statement value, in days, when auto-reenrollment should start before expiration.

Options **percentage**—Percentage for the reenroll trigger time.
Range: 1 through 99

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Auto-Reenrollment of a Router Certificate on page 191](#)
- [auto-re-enrollment on page 679](#)

refresh-interval

Syntax	<code>refresh-interval <i>number-of-hours</i>;</code>
Hierarchy Level	<code>[edit security pki ca-profile <i>ca-profile-name</i> revocation-check <i>crl</i>]</code>
Release Information	Statement introduced in Junos OS Release 8.1.
Description	(Adaptive services interfaces only) Specify the amount of time between certificate revocation list (CRL) updates.
Options	<p><i>number-of-hours</i>—Time interval, in hours, between CRL updates.</p> <p>Range: 0 through 8784</p> <p>Default: 24</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Certificate Revocation List on page 188 • crl on page 713

re-generate-keypair

Syntax	<code><re-generate-keypair>;</code>
Hierarchy Level	<code>[edit security pki auto-re-enrollment certificate-id]</code>
Release Information	Statement introduced in Junos OS Release 8.5.
Description	(Optional) Automatically generate a new key pair when auto-reenrolling a router certificate. If this statement is not configured, the current key pair is used.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Auto-Reenrollment of a Router Certificate on page 191 • auto-re-enrollment on page 679

remote (Host VPN)

Syntax	<pre>remote { id <i>remote-id</i>; }</pre>
Hierarchy Level	[edit security host-vpn]
Release Information	Statement introduced in Junos OS Evolved Release 18.3R1.
Description	Configure the identity details for authenticating the remote device during IKE negotiations.
Options	id <i>remote-id</i> —Specify the remote IKE identity to use when authenticating the host-to-host VPN connection. The identity can be an IP address, a domain name, or an e-mail address. This identity matches the local identity.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

remote-id

Syntax

```
remote-id {
  host-name host-name;
  mac (Option 82);
  prefix ( hostname | mac | none);
  use-interface-description (logical | device);
  use-string string;
}
```

- Hierarchy Level**
- For platforms with Enhanced Level 2 Software (ELS):

```
[edit vlans vlan-name forwarding-options dhcp-security option-82]
```

- For platforms without ELS:

```
[edit ethernet-switching-options secure-access-port vlan (all | vlan-name)
  dhcp-option82],
[edit forwarding-options helpers bootp dhcp-option82],
[edit forwarding-options helpers bootp interface interface-name dhcp-option82]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
 Statement introduced in Junos OS Release 11.3 for the QFX Series.
 Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security option-82]**
 introduced in Junos OS Release 13.2X50-D10. (See *Using the Enhanced Layer 2 Software CLI* for information about ELS.)

Description

Insert the **remote-id** suboption of DHCP option 82 (also known as the DHCP relay agent information option) in DHCP request packet headers before forwarding or relaying requests to a DHCP server. This suboption provides a trusted identifier for the host system that has forwarded or relayed requests to the server.

The remaining statements are explained separately, and their availability depends on the hierarchy level at which the **remote-id** suboption is specified, as follows:

- The statement **prefix**, is *not* supported at the **[edit vlans *vlan-name* forwarding-options dhcp-security option-82]** hierarchy level.
- The statement **host-name** is supported *only* at the **[edit vlans *vlan-name* forwarding-options dhcp-security option-82]** hierarchy level.

Default

If the **remote-id** statement is not explicitly set, no remote ID value is inserted in the DHCP request packet header.

If the **remote-id** statement is explicitly set, but is not qualified by a keyword, the following are true:

- At the **[edit vlans *vlan-name* forwarding-options dhcp-security]** hierarchy level, the default keyword value is *interface-name*.

- At all other hierarchy levels, the default value of the **remote-id** keyword is the MAC address of the switch.



NOTE: When you configure **remote-id**, **circuit-id** is also enabled, even if you do not explicitly configure **circuit-id**.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation • [Example: Setting Up DHCP Option 82 on page 433](#)
 • RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>

remote-id (MX Series)

Syntax	<pre>remote-id { host-name; use-interface-description (logical device); use-string <i>string</i>; }</pre>
Hierarchy Level	[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82]
Release Information	Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	<p>Insert the remote-id suboption of DHCP option 82 (also known as the DHCP relay agent information option) in DHCP request packet headers before forwarding or relaying requests to a DHCP server. This suboption provides a trusted identifier for the host system that has forwarded or relayed requests to the server.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Default	<p>If the remote-id statement is not explicitly set, no remote ID value is inserted in the DHCP request packet header.</p> <p>If the remote-id statement is explicitly set, but is not qualified by a keyword, the default value is the device MAC address.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring DHCP Option 82 on a Router with Bridge Domain on page 437 • RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046

replay-protect

Syntax	<pre>replay-protect { replay-window-size <i>number-of-packets</i>; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Enable replay protection for MACsec.</p> <p>A replay window size specified using the replay-window-size <i>number-of-packets</i> statement must be specified to enable replay protection.</p>
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228

replay-protect (MX Series)

Syntax	<pre>replay-protect { replay-window-size <i>number-of-packets</i>; }</pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Enable replay protection for MACsec.</p> <p>A replay window size specified using the replay-window-size <i>number-of-packets</i> statement must be specified to enable replay protection.</p>
Options	The remaining statements are explained separately.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

remote-traffic-selector

Syntax	<pre>remote-traffic-selector { (ipv4-prefix <i>ipv4-prefix</i> ipv6-prefix <i>ipv6-prefix</i>); port <i>port</i>; protocol <i>protocol</i>; }</pre>
Hierarchy Level	[edit security host-vpn connections <i>connection-name</i> children <i>child-name</i>]
Release Information	Statement introduced in Junos OS Evolved Release 18.3R1.
Description	Configure the remote IPsec traffic to be protected by the child security association. A traffic selector is a traffic filter that defines and identifies the traffic flow permitted between two systems (a specified pair of local and remote addresses) that have IPsec protection.
Options	<p>(ipv4-prefix <i>ipv4-prefix</i> ipv6-prefix <i>ipv6-prefix</i>)—Specify traffic to be protected by the child security association using either IPv4 or IPv6 with a prefix. The prefix allows for specifying more general traffic.</p> <p>port <i>port</i>—Specify the port to protect by number or name. For example, port 21 and port ftp refer to the same port.</p> <p>protocol <i>protocol</i>—Specify the protocol to protect by number or name. For example, protocol 6 and protocol tcp refer to the same protocol.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>

replay-window-size (MX Series)

Syntax	<code>replay-window-size <i>number-of-packets</i>;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> replay-protect]</code>
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specifies the size of the replay protection window.</p> <p>This statement has to be configured to enable replay protection.</p> <p>When MACsec is enabled on an Ethernet link, an ID number is assigned to each packet entering the link. The ID number of the packet is checked by the receiving interface after the packet has traversed the MACsec-enabled link.</p> <p>When replay protection is enabled, the sequence of the ID number of received packets are checked. If the packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.</p> <p>Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.</p> <p>Replay protection should not be enabled in cases where packets are expected to arrive out of order.</p>
Default	Replay protection is disabled.
Options	<p><i>number-of-packets</i>—Specifies the size of the replay protection window, in packets.</p> <p>When this variable is set to 0, all packets that arrive out-of-order are dropped.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

replay-window-size

Syntax	<code>replay-window-size <i>number-of-packets</i>;</code>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i> replay-protect]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specifies the size of the replay protection window.</p> <p>This statement has to be configured to enable replay protection.</p> <p>When MACsec is enabled on an Ethernet link, an ID number is assigned to each packet entering the link. The ID number of the packet is checked by the receiving interface after the packet has traversed the MACsec-enabled link.</p> <p>When replay protection is enabled, the sequence of the ID number of received packets are checked. If the packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.</p> <p>Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.</p> <p>Replay protection should not be enabled in cases where packets are expected to arrive out of order.</p>
Default	Replay protection is disabled.
Options	<p><i>number-of-packets</i>—Specifies the size of the replay protection window, in packets.</p> <p>When this variable is set to 0, all packets that arrive out-of-order are dropped.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring MACsec on EX, SRX and Fusion Devices on page 228

retry (Adaptive Services Interface)

Syntax	<code>retry <i>number-of-attempts</i>;</code>
Hierarchy Level	<code>[edit security pki ca-profile <i>ca-profile-name</i> enrollment]</code>
Release Information	Statement introduced in Junos OS Release 7.5.
Description	(Adaptive services interfaces only) Specify how many times a router can resend a digital certificate request.
Options	<i>number-of-attempts</i> —Number of enrollment retries. Range: 0 through 100 Default: 0
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Enrollment Properties on page 187• enrollment on page 752

retry-interval

Syntax	<code>retry-interval <i>seconds</i>;</code>
Hierarchy Level	<code>[edit security pki ca-profile <i>ca-profile-name</i> enrollment]</code>
Release Information	Statement introduced in Junos OS Release 7.5.
Description	(Adaptive services interfaces only) Specify the amount of time the router should wait between enrollment retries.
Options	<i>seconds</i> —Time interval, in seconds, between enrollment retries. Range: 0 through 3600 Default: 0
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Enrollment Properties on page 187• enrollment on page 752

revocation-check

Syntax	<pre> revocation-check { disable; crl { refresh-interval <i>number-of-hours</i>; url { <i>url-name</i>; } } } </pre>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	Specify the method to verify revocation status of digital certificates for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M Series and T Series routers.
Options	<p>disable—Disable verification of status of digital certificates. Use disable temporarily in cases where a certificate authority (CA) server is unreachable and certificate cannot be renewed or if the certificate download fails.</p> <p>crl—Only certificate revocation list (CRL) is supported. A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis. By default, crl is enabled.</p> <p>The PKID process might fail after RGO failover on the new node causing all the IPsec VPNs using the public key infrastructure (PKI) to go down when:</p> <ul style="list-style-type: none"> • A local certificate used for IPsec VPN is revoked by the Certificate Authority (CA). • Certificate revocation list (CRL) check is disabled. • CRL is not cleared. <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Certificate Revocation List on page 188

router-advertisement-guard

```
Syntax router-advertisement-guard {
  interface interface-name {
    mark-interface (trusted | block);
    policy policy-name (stateful | stateless);
  }
  vlans (vlan-name | all) {
    policy policy-name (stateful | stateless);
  }
  policy policy-name {
    accept {
      match-list {
        match-criteria {
          (match-all | match-any);
        }
        prefix-list-name prefix-list-name;
        source-ip-address-list address-list-name;
        source-mac-address-list address-list-name;
      }
      match-option {
        hop-limit {
          (maximum | minimum) value;
        }
        managed-config-flag;
        other-config-flag;
        router-preference (high | low | medium);
      }
    }
    discard {
      prefix-list-name prefix-list-name;
      source-ip-address-list address-list-name;
      source-mac-address-list address-list-name;
    }
  }
}
```

Hierarchy Level [edit forwarding-options [access-security](#)]

Release Information Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.
Statement introduced in Junos OS Release 16.1 for EX Series switches.

Description Configure IPv6 Router Advertisement (RA) guard. In an IPv6 deployment, RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in a policy. The policy can be either an accept policy or a discard policy. When RA guard is enabled by using an accept policy, any RA messages that match the conditions defined in the policy are forwarded, and RA messages that do not match the conditions are dropped. When RA guard is enabled by using a discard

policy, any RA messages that match the conditions are dropped, and RA messages that do not match the conditions are forwarded.

You can enable RA guard on an interface or on a VLAN. You must first configure a policy at the `[edit forwarding-options access-security router-advertisement-guard]` hierarchy level. The policy is then applied to an interface at the `[edit forwarding-options access-security router-advertisement-guard interface interface-name]` hierarchy level, or to a VLAN at the `[edit forwarding-options access-security router-advertisement-guard vlan vlan-name]` hierarchy level.



NOTE: If you apply an RA guard policy on an interface, you must enable RA guard on the VLAN that is associated with that interface using the `vlan` statement at the `[edit forwarding-options access-security router-advertisement-guard]` hierarchy level.

You can configure RA guard to be stateless or stateful. Stateless RA guard enables a switch to examine incoming RA messages and filter each message on the basis of whether it matches the conditions configured in the policy. For example, an interface can be statically configured to forward RA messages only from predefined sources. Stateful RA guard enables a switch to learn about legitimate senders of RA messages and store this information, which is used to validate senders of subsequent RA messages. For example, an interface that is in the learning state and receives RA messages from legitimate senders dynamically transitions to the forwarding state, in which RA messages from valid senders are forwarded to their destination.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514
------------------------------	---

routing-instance-name

Syntax	routing-instance-name;
Hierarchy Level (EX Series)	[edit vlans forwarding-options dhcp-security option-82 circuit-id prefix]
Hierarchy Level (MX Series)	[edit bridge-domains <i>bridge domain name</i> forwarding-options dhcp-security option-82 circuit-id prefix]
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	Specify that the routing instance name be included within the optional prefix for the circuit ID suboption in the DHCP option 82 information that is inserted by the switch into the packet header of a DHCP request before it forwards or relays the request to a DHCP server.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Setting Up DHCP Option 82 on the Switch with No Relay (ELS) on page 439 • Configuring DHCP Option 82 on a Router with Bridge Domain on page 437

routing-instance-name (circuit-id)

Syntax	routing-instance--name;
Hierarchy Level	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 circuit-id prefix]
Release Information	Statement introduced in Junos OS Release 13.2 for EX Series switches.
Description	Specify that the routing instance name used by the VLAN is included with the circuit ID suboption in the DHCP option 82 information that is inserted by the switch into the packet header of a DHCP request before it forwards or relays the request to a DHCP server
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Setting Up DHCP Option 82 on the Switch with No Relay (ELS) on page 439 • Understanding DHCP Option 82 on page 429

rpf-check

List of Syntax	Syntax (MX Series, SRX Series, M Series, T Series, PTX Series) on page 977 Syntax (EX Series and QFX Series) on page 977
Syntax (MX Series, SRX Series, M Series, T Series, PTX Series)	<pre>rpf-check { fail-filter <i>filter-name</i>; mode loose; }</pre>
Syntax (EX Series and QFX Series)	<pre>rpf-check;</pre>
Hierarchy Level (MX Series, SRX Series, M Series, T Series, PTX Series)	<pre>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>inet</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>inet6</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>inet</i>] [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>inet6</i>]</pre>
Hierarchy Level (EX Series and QFX Series)	<pre>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>inet</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>inet6</i>]</pre>
Release Information	<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 the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Support for interface ps0 (pseudowire subscriber logical interface device) added in Junos OS Release 15.1.</p>
Description	<p>Enable a reverse-path forwarding (RPF) check on unicast traffic.</p> <p>On EX3200 and EX4200 switches, enable a reverse-path forwarding (RPF) check on unicast traffic (except ECMP packets) on all ingress interfaces.</p> <p>On EX4300 switches, enable a reverse-path forwarding (RPF) check on unicast traffic, including ECMP packets, on all ingress interfaces.</p> <p>On EX8200 and EX6200 switches, enable an RPF check on unicast traffic, including ECMP packets, on the selected ingress interfaces.</p> <p>On QFX Series switches, enable an RPF check on unicast traffic on the selected ingress interfaces. ECMP packets are checked by QFX5000 Series switches only.</p> <p>The mode statement is explained separately.</p>
Default	<p>Unicast RPF is disabled on all interfaces.</p>

Options	fail-filter —A filter to evaluate when packets are received on the interface. If the RPF check fails, this optional filter is evaluated. If the fail filter is not configured, the default action is to silently discard the packet.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Unicast RPF Strict Mode on page 591• Configuring Unicast RPF Loose Mode on page 593• Configuring a Pseudowire Subscriber Logical Interface Device• Example: Configuring Unicast RPF (On a Switch) on page 598

secret

Syntax	<code>secret <i>secret-data</i>;</code>
Hierarchy Level	<code>[edit security authentication-key-chains key-chain <i>key-chain-name</i> key <i>key</i>]</code>
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for the BFD protocol introduced in Junos OS Release 9.6. Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches. Support for IS-IS introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 11.3 for QFX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify a password in encrypted text or plain text format. The secret password always appears in encrypted format.
Options	secret-data —Password to use; it can include spaces if the character string is enclosed in quotation marks.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols• Example: Configuring BFD Authentication for Securing Static Routes• Example: Configuring Hitless Authentication Key Rollover for IS-IS

secure-access-port

```
Syntax secure-access-port {
    dhcp-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    dhcpv6-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    interface (all | interface-name) {
        allowed-mac {
            mac-address-list;
        }
        (dhcp-trusted | no-dhcp-trusted);
        fcoe-trusted;
        mac-limit limit action (drop | log | none | shutdown);
        no-allowed-mac-log;
        persistent-learning;
        static-ipip-address {
            vlan vlan-name;
            mac mac-address;
        }
        static-ipv6ip-address {
            vlan vlan-name;
            mac mac-address;
        }
        }
        voip-mac-exclusive;
        (dhcp-trusted | no-dhcp-trusted);
    }
    vlan (all | vlan-name) {
        (arp-inspection | no-arp-inspection) [
            forwarding-class class-name;
        ]
        dhcp-option82 {
            circuit-id {
                prefix hostname;
                use-interface-description;
                use-vlan-id;
            }
            remote-id {
                prefix hostname | mac | none;
                use-interface-description;
                use-string string;
            }
            vendor-id <string>;
        }
        (examine-dhcp | no-examine-dhcp) {
            forwarding-class class-name;
        }
    }
}
```

```

(examine-dhcpv6 | no-examine-dhcpv6) {
    forwarding-class class-name;
}
examine-fip {
    fc-map fc-map-value;
}
(ip-source-guard | no-ip-source-guard);
(ipv6-source-guard | no-ipv6-source-guard);
mac-move-limit limit action (drop | log | none | shutdown);
}
(neighbor-discovery-inspection | no-neighbor-discovery-inspection);
no-option37;
}
}

```

Hierarchy Level [edit [ethernet-switching-options](#)]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for IPv6 introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Configure port security features, including MAC limiting, dynamic ARP inspection, whether interfaces can receive DHCP responses, DHCP snooping, IP source guard, DHCP option 82, MAC move limiting, and FIP snooping.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

- Related Documentation**
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
 - [Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks on page 406](#)
 - [Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 467](#)
 - [Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443](#)
 - [Example: Configuring an FCoE Transit Switch](#)

secure-channel

Syntax	<pre> secure-channel <i>secure-channel-name</i> { direction (inbound outbound); encryption (MACsec); id { mac-address <i>mac-address</i>; port-id <i>port-id-number</i>; } offset (0 30 50); security-association <i>security-association-number</i> { key <i>key-string</i>; } } </pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Create and configure a secure channel to enable and configure MACsec when MACsec is enabled using static secure association key (SAK) security mode.</p> <p>You do not need to use this option to enable MACsec using static connectivity association key (CAK) security mode. All configuration for MACsec using static CAK security mode is done inside of the connectivity association but outside of the secure channel. When MACsec is enabled using static CAK security mode, an inbound and an outbound secure channel—neither of which is user-configurable—is automatically created within the connectivity association.</p>
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring MACsec on EX, SRX and Fusion Devices on page 228

secure-channel

Syntax	<pre> secure-channel <i>secure-channel-name</i> { direction (inbound outbound); encryption (MACsec); id { mac-address <i>mac-address</i>; port-id <i>port-id-number</i>; } offset (0 30 50); security-association <i>security-association-number</i> { key <i>key-string</i>; } } </pre>
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Create and configure a secure channel to enable and configure MACsec when MACsec is enabled using static secure association key (SAK) security mode.</p> <p>You do not need to use this option to enable MACsec using static connectivity association key (CAK) security mode. All configuration for MACsec using static CAK security mode is done inside of the connectivity association but outside of the secure channel. When MACsec is enabled using static CAK security mode, an inbound and an outbound secure channel—neither of which is user-configurable—is automatically created within the connectivity association.</p>
Options	The remaining statements are explained separately.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

security

```
Syntax security {
  authentication-key-chains {
    key-chain key-chain-name {
      key key {
        secret secret-data;
        start-time yyyy-mm-dd.hh:mm:ss;
      }
    }
  }
  certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority ca-profile-name {
      ca-name ca-identity;
      crl file-name;
      encoding (binary | pem);
      enrollment-url url-name;
      file certificate-filename;
      ldap-url url-name;
    }
    enrollment-retry attempts;
    local certificate-filename {
      certificate-key-string;
      load-key-file key-file-name;
    }
    maximum-certificates number;
    path-length certificate-path-length;
  }
  ssh-known-hosts {
    host {
      fetch-from-server host-name;
      load-key-file file-name;
    }
  }
  traceoptions {
    file filename <files number> <size size>;
    flag flag;
    level level;
    no-remote-trace
  }
}
```

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

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure security services. Most of the configuration statements do not have default values. If you do not specify an identifier for a statement that does not have a default value, you cannot commit the configuration.

**Required Privilege
Level**

**Related
Documentation**

security-association

Syntax	<pre>security-association <i>security-association-number</i> { key <i>key-string</i>; }</pre>
Hierarchy Level	[edit security macsec connectivity-association connectivity-association-name secure-channel secure-channel-name]
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specifies the number of one of the security associations in the secure channel when MACsec is enabled using static secure association key (SAK) security mode. Because SAKs are created by the key server when MACsec is enabled using static connectivity association key (CAK) security mode, the security-association statement is not used when enabling MACsec using static CAK security mode.</p> <p>You must configure at least two security associations to enable MACsec using static SAK security mode. MACsec initially establishes a secure connection when a security association number and key match on both ends of an Ethernet link. After a certain number of Ethernet frames are securely transmitted across the Ethernet link, MACsec automatically rotates to a new security association with a new security association number and key to maintain the secured Ethernet link. This rotation continues each time a certain number of Ethernet frames are securely transmitted across the secured Ethernet link, so you must always configure MACsec to have at least two security associations.</p>
Default	No security keys are configured, by default.
Options	<p><i>security-association-number</i>—Specifies the security association number and creates the SAK.</p> <p>The security association number is a whole number between 0 and 3. You can configure two security associations in a secure channel when enabling MACsec using static security keys.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring MACsec on EX, SRX and Fusion Devices on page 228

security-association (Junos OS)

```
Syntax security-association sa-name {
  dynamic {
    ipsec-policy policy-name;
    replay-window-size (32 | 64);
  }
  manual {
    direction (inbound | outbound | bi-directional) {
      authentication {
        algorithm (hmac-sha1-96 | hmac-sha2-256);
        key (ascii-text key | hexadecimal key);
      }
      auxiliary-spi auxiliary-spi-value;
      encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
      }
      protocol ( ah | esp | bundle);
      spi spi-value;
    }
    mode (tunnel | transport);
  }
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.



NOTE: You must configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Description Configure an IPsec security association.

Options ***sa-name***—Name of the security association.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege
Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Security Associations for IPsec on an ES PIC on page 37](#)

security-association (Junos-FIPS Software)

Syntax

```
security-association sa-name {
  dynamic {
    ipsec-policy policy-name;
    replay-window-size (32 | 64);
  }
  manual {
    direction (inbound | outbound | bi-directional) {
      authentication {
        algorithm (hmac-sha1-96 | hmac-sha2-256);
        key (ascii-text key | hexadecimal key);
      }
      auxiliary-spi auxiliary-spi-value;
      encryption {
        algorithm 3des-cbc;
        key (ascii-text key | hexadecimal key);
      }
      protocol ( ah | esp | bundle);
      spi spi-value;
    }
    mode (tunnel | transport);
  }
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.



NOTE: We recommend that you configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Description Configure an IPsec security association.

Options *sa-name*—Name of the security association.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

security-mode

Syntax	<code>security-mode <i>security-mode</i>;</code>
Hierarchy Level	<code>[edit security <i>macsec connectivity-association</i> <i>connectivity-association-name</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 13.2X50-D15.</p> <p>The dynamic security mode option was introduced in Junos OS Release 14.1X53-D10.</p> <p>Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.</p>
Description	<p>Configure the MACsec security mode for the connectivity association.</p> <p>We recommend enabling MACsec on switch-to-switch Ethernet links using static connectivity association key (CAK) security mode. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available when you enable MACsec using static CAK security mode.</p>
Options	<p><i>security-mode</i>—Specifies the MACsec security mode. Options include:</p> <ul style="list-style-type: none"> • dynamic—Dynamic mode. <p>Dynamic security mode is used to enable MACsec on switch-to-host Ethernet links. In dynamic mode, a master key is retrieved from a RADIUS server by a switch and a host as part of the AAA handshake in separate transactions. The MKA protocol is enabled when the master key is exchanged between the switch and the host.</p> <ul style="list-style-type: none"> • static-cak—Static connectivity association key (CAK) mode. <p>Static CAK security mode is used to enable MACsec on switch-to-switch Ethernet links. In static-cak mode, the switch at one end of the point-to-point link acts as the key server and regularly transmits a randomized key using a process that does not transmit any traffic outside of the MACsec-secured point-to-point link.</p> <ul style="list-style-type: none"> • static-sak—Static secure association key (SAK) mode. <p>Static SAK security mode is used to enable MACsec on switch-to-switch Ethernet links. In static-sak mode, one of two user-configured security keys is used to secure the point-to-point link. The two security keys are regularly rotated.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

**Related
Documentation**

- [Configuring MACsec on EX, SRX and Fusion Devices on page 228](#)

show ddos-protection protocols culprit-flows

Syntax	show ddos-protection protocols <i><protocol-group (aggregate packet-type)> culprit-flows</i>
Release Information	<p>Command introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	Display culprit flow information for protocol groups or individual packet types.
Options	<p>none—Display information for all protocol groups and packet types.</p> <p>brief detail —(Optional) Display the specified level of output.</p> <p>fpc-slot—(Optional) Display information for the specified Flexible PIC Concentrator (FPC) slot.</p> <p>Default: system-wide, that is; include all the FPC slots.</p> <p>Range: 0 through 2</p> <p>summary—(Optional) Display flow information summary.</p> <p>aggregate—(Optional) Display DDoS protection information for the aggregate policer. The aggregate option is available for all protocol groups.</p> <p>packet-type—(Optional) Display information for the specified packet type in the protocol group. The available packet types vary by protocol group.</p> <p>See show ddos-protection protocols for a list of available packet types.</p> <p>protocol-group—(Optional) Display information for a particular protocol group.</p> <p>See show ddos-protection protocols for a list of available groups.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear ddos-protection protocols on page 1077 • show ddos-protection protocols on page 1132 • show ddos-protection protocols flow-detection on page 997 • show ddos-protection protocols parameters on page 1153 • show ddos-protection protocols statistics on page 1160 • show ddos-protection protocols violations on page 1171

List of Sample Output

- [show ddos-protection protocols culprit-flows brief on page 992](#)
- [show ddos-protection protocols culprit-flows for all protocols on page 992](#)
- [show ddos-protection protocols culprit-flows detail \(Specific Protocol Group\) on page 993](#)
- [show expanded format for dhcpv4 discover packet type on page 993](#)
- [show dhcpv4 flow detection information on page 994](#)
- [show dhcpv4 flow detection information in brief format on page 995](#)
- [show global statistics on page 996](#)
- [show ddos-protection protocols culprit-flows fpc-slot on page 996](#)

Output Fields Table 38 on page 991 lists the output fields for the **show ddos-protection protocols culprit-flows** command. Output fields are listed in the approximate order in which they appear.

Table 38: show ddos-protection protocols culprit-flows Output Fields

Field Name	Field Description	Level of Output
Currently tracked flows	Number of active flows that are being tracked as culprit flows by flow detection.	All levels
Total detected flows	Total number of culprit flows that have been detected, including those that have recovered or timed out.	All levels
Protocol Group	Name of protocol group.	detail
Packet type	Name of packet type in protocol group.	detail
Arriving Interface	Logical interface on which the traffic flow arrived.	detail
Aggr Flow Id level	Shows the flow_id, such as flow_id 0001000000000022	detail
Source Address MAC or IP	Source address of the traffic flow, either a MAC address or an IP address.	detail
Destination Address MAC or IP	Destination address of the traffic flow, either a MAC address or an IP address.	detail
Source Port	Source port number.	detail
Destination Port	Destination port number.	detail
pps	Rate of the traffic flow in packets per second.	brief
Rate	Rate of the traffic flow in packets per second.	detail
pkts	Number of packets received in the traffic flow.	brief
received packets	Number of packets received in the traffic flow.	detail

Table 38: show ddos-protection protocols culprit-flows Output Fields (continued)

Field Name	Field Description	Level of Output
Additional information	Flow ID numbers automatically assigned to flow, with embedded slot ID. The flow ID is prefixed by sub , ifl , or ifd , which indicate the subscriber, logical interface, and physical interface flow aggregation levels. Timestamp that identifies when the flow arrived on the interface.	detail

Sample Output

show ddos-protection protocols culprit-flows brief

```

user@host> show ddos-protection protocols culprit-flows brief

Currently tracked flows: 1000, Total detected flows: 1000
Protocol Packet Arriving Source Address
group type Interface MAC or IP
ndpv6 router-adv ge-1/1/0.0

2001:db8::03d4 sub:0001000000000384 2015-03-13 00:21:07 PDT pps:72 pkts:547072
ndpv6 router-adv ge-1/1/0.0
2001:db8::013f
sub:0001000000000385 2015-03-13 00:21:07 PDT pps:72 pkts:552704
ndpv6 router-adv ge-1/1/0.0
2001:db8::02e4
sub:0001000000000386 2015-03-13 00:21:07 PDT pps:72 pkts:726784
ndpv6 router-adv ge-1/1/0.0
2001:0db8::0102
sub:0001000000000387 2015-03-13 00:21:07 PDT pps:72 pkts:762880

```

show ddos-protection protocols culprit-flows for all protocols

```

user@host> show ddos-protection protocols culprit-flows

Currently tracked flows: 1003, Total detected flows: 1003
Protocol group Packet type Arriving Interface Source Address MAC or IP
pppoe padi ge-1/3/0.0 00:10:94:00:00:02
flow_id:0001000000000003 2017-09-12 16:48:58 PDT pps:2000 pkts:153606295
dhcpv4 discover ge-1/2/0.100 -- -- --
flow_id:0001000000000000 2017-09-12 16:48:56 PDT pps:1000 pkts:76805613
dhcpv4 discover ge-1/2/0.100 192.85.1.2
flow_id:0001000000000001 2017-09-12 16:48:56 PDT pps:1000 pkts:76805603
bfd aggregate ge-1/2/0.100 192.85.1.2
flow_id:0001000000000002 2017-09-12 16:48:57 PDT pps:30 pkts:2303747286
bfd aggregate ge-1/2/0.100 192.85.2.249
flow_id:0001000000000004 2017-09-13 14:08:53 PDT pps:30 pkts:203
bfd aggregate ge-1/2/0.100 192.85.1.36
flow_id:0001000000000005 2017-09-13 14:08:53 PDT pps:30 pkts:204
bfd aggregate ge-1/2/0.100 192.85.1.211
flow_id:0001000000000006 2017-09-13 14:08:53 PDT pps:30 pkts:204
bfd aggregate ge-1/2/0.100 192.85.4.79
flow_id:0001000000000007 2017-09-13 14:08:53 PDT pps:30 pkts:205
bfd aggregate ge-1/2/0.100 192.85.4.219
flow_id:0001000000000008 2017-09-13 14:08:53 PDT pps:30 pkts:204
bfd aggregate ge-1/2/0.100 192.85.2.134
flow_id:0001000000000009 2017-09-13 14:08:53 PDT pps:30 pkts:204

```

show ddos-protection protocols culprit-flows detail (Specific Protocol Group)

```

user@host> show ddos-protection protocols pppoe culprit-flows detail

Currently tracked flows: 2, Total detected flows: 1000
Protocol group Packet type Arriving Interface Aggr Flow Id level
pppoe      padi      ge-1/1/0.1      flow_id 0001000000000022
Ethertype: 0x0 outer-vlan: 100 inner-vlan: ---
Source Address: 00:10:94:00:00:02
Destination Address: FF:FF:FF:FF:FF:FF
Found at: 2017-10-07 07:11:27 PDT
Last Violation: 2017-10-07 07:43:24 PDT
Rate: 9995 pps received packets: 18546724

ppoe      padi      ge-1/1/0.1      flow_id 000100000000031c
Ethertype: 0x0 outer-vlan: 100 inner-vlan: ---
Source Address: 00:10:94:00:00:03
Destination Address: FF:FF:FF:FF:FF:FF
Found at: 2017-10-07 07:11:27 PDT
Last Violation: 2017-10-07 07:43:24 PDT
Rate: 9995 pps received packets: 18546715

```

```

user@host> show ddos-protection protocols pppoe culprit-flows detail

Currently tracked flows: 1, Total detected flows: 1000
Protocol Packet Arriving Aggr Flow Id
group type Interface level
pppoe padi ge-1/1/0.1 sub 0001000000000022
Ethertype: 0x0 outer-vlan: 100 inner-vlan: ---
Source Address: 2001:db8::02
Destination Address: 2001:db8::FF
Found at: 2014-10-07 07:11:27 PDT
Last Violation: 2014-10-07 07:43:24 PDT
Rate: 9995 pps received packets: 18546724

```

```

user@host> show ddos-protection protocols ndpv6 culprit-flows detail

Currently tracked flows: 1, Total detected flows: 1
Protocol Packet Arriving Aggr Flow Id
group type Interface level
ndpv6 router-sol ge-1/1/0.2 sub 0001000000000001
Source Address: 2001:db8::03
Destination Address: 2001:0db8::0111
Type: 133 Code: 0
Found at: 2014-10-23 11:55:20 PDT
Last Violation: 2014-10-23 11:55:21 PDT
Rate: 30000 pps received packets: 43469

```

show expanded format for dhcpv4 discover packet type

```

user@host> show ddos-protection protocols dhcpv4 discover

Currently tracked flows: 0, Total detected flows: 0
* = User configured value Protocol Group: DHCPv4

Packet type: discover (DHCPv4 DHCPDISCOVER) Individual policer configuration:
Bandwidth: 500 pps
Burst: 500 packets
Priority: Low
Recover time: 300 seconds Enabled: Yes
Bypass aggregate: No

```

```

Flow detection configuration:
  Detection mode: Automatic Detect time: 3 seconds
  Log flows: Yes
  Recover time: 60 seconds
  Timeout flows: No
  Timeout time: 300 seconds
  Flow aggregation level configuration:
Aggregation level Detection mode Control mode Flow rate
Subscriber Automatic Drop 10 pps
Logical interface Automatic Drop 10 pps
Physical interface Automatic Drop 500 pps
System-wide information: Bandwidth is never violated
Received: 0
Arrival rate: 0 pps
Dropped: 0
Max arrival rate: 0 pps
Routing Engine information:
  Bandwidth: 500 pps, Burst: 500 packets, enabled Policer is never violated
  Received: 0 Arrival rate: 0 pps
  Dropped: 0 Max arrival rate: 0 pps Dropped by aggregate policer: 0
FPC slot 1 information:
  Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled Policer is never
violated
  Received: 0 Arrival rate: 0 pps
  Dropped: 0 Max arrival rate: 0 pps Dropped by aggregate policer: 0
  Dropped by flow suppression: 0

```

show dhcpv4 flow detection information

```
user@host> show ddos-protection protocols dhcpv4 flow-detection
```

```

Packet types: 19, Modified: 0
* = User configured value Protocol Group: DHCPv4
Packet type: aggregate
Flow detection configuration:
  Detection mode: Automatic
  Detect time: 3 seconds
  Log flows: Yes
  Recover time: 60 seconds
  Timeout flows: No
  Timeout time: 300 seconds
  Flow aggregation level configuration:
Aggregation level Detection mode Control mode Flow rate
Subscriber Automatic Drop 10 pps
Logical interface Automatic Drop 10 pps
Physical interface Automatic Drop 5000 pps

Packet type: unclassified
Flow detection configuration:
  Detection mode: Automatic
  Detect time: 3 seconds
  Log flows: Yes
  Recover time: 60 seconds
  Timeout flows: No
  Timeout time: 300 seconds
  Flow aggregation level configuration:
Aggregation level Detection mode Control mode Flow rate
Subscriber Automatic Drop 10 pps
Logical interface Automatic Drop 10 pps
Physical interface Automatic Drop 300 pps

```

```

Packet type: discover
Flow detection configuration:
Detection mode: Automatic
Detect time: 3 seconds
Log flows: Yes
Recover time: 60 seconds
Timeout flows: No
Timeout time: 300 seconds
Flow aggregation level configuration:
Aggregation level Detection mode Control mode Flow rate
Subscriber Automatic Drop 10 pps
Logical interface Automatic Drop 10 pps
Physical interface Automatic Drop 500 pps

Packet type: offer
Flow detection configuration:
Detection mode: Automatic
Detect time: 3 seconds
Log flows: Yes
Recover time: 60 seconds
Timeout flows: No
Timeout time: 300 seconds
Flow aggregation level configuration:
Aggregation level Detection mode Control mode Flow rate
Subscriber Automatic Drop 10 pps
Logical interface Automatic Drop 10 pps

```

show dhcpv4 flow detection information in brief format

```
user@host> show ddos-protection protocols dhcpv4 flow-detection brief
```

```

Packet types: 19, Modified: 0
* = User configured value

```

```

Detection mode(Op): a = automatic Flow control mode(Fc): d = drop o = on k = keep
x = off p = police

```

```

Protocol Packet Op Policer Aggr lvl Op:Fc:BW(pps)Log Time
group type mode BW(pps) sub ifl ifd flow out

```

```

dhcpv4 aggregate auto 5000 a:d:10 a:d:10 a:d:5000 Yes No
dhcpv4 unclass.. auto 300 a:d:10 a:d:10 a:d:300 Yes No
dhcpv4 discover auto 500 a:d:10 a:d:10 a:d:500 Yes No
dhcpv4 offer auto 1000 a:d:10 a:d:10 a:d:1000 Yes No
dhcpv4 request auto 1000 a:d:10 a:d:10 a:d:1000 Yes No
dhcpv4 decline auto 500 a:d:10 a:d:10 a:d:500 Yes No
dhcpv4 ack auto 500 a:d:10 a:d:10 a:d:500 Yes No
dhcpv4 nak auto 500 a:d:10 a:d:10 a:d:500 Yes No
dhcpv4 release auto 2000 a:d:10 a:d:10 a:d:2000 Yes No
dhcpv4 inform auto 500 a:d:10 a:d:10 a:d:500 Yes No
dhcpv4 renew auto 2000 a:d:10 a:d:10 a:d:2000 Yes No
dhcpv4 forcerenew auto 2000 a:d:10 a:d:10 a:d:2000 Yes No
dhcpv4 leasequery auto 2000 a:d:10 a:d:10 a:d:2000 Yes No
dhcpv4 leaseuna.. auto 2000 a:d:10 a:d:10 a:d:2000 Yes No
dhcpv4 leaseunk.. auto 2000 a:d:10 a:d:10 a:d:2000 Yes No
dhcpv4 leaseact.. auto 2000 a:d:10 a:d:10 a:d:2000 Yes No
dhcpv4 bootp auto 300 a:d:10 a:d:10 a:d:300 Yes No

```

```
dhcpv4  no-msgtype  auto 1000 a:d:10 a:d:10 a:d:1000 Yes No
dhcpv4  bad-pack..  auto 0   a:d:10 a:d:10 a:d:0   Yes No
```

show global statistics

```
user@host> show ddos-protection statistics
```

```
DDOS protection global statistics:
  Policing on routing engine: Yes
  Policing on FPC: Yes
  Flow detection: No
  Logging: Yes
  Policer violation report rate: 100
  Flow report rate: 100
  Currently violated packet types: 0
  Packet types have seen violations: 0
  Total violation counts: 0
  Currently tracked flows: 0
  Total detected flows: 0
```

show ddos-protection protocols culprit-flows fpc-slot

```
user@host> show ddos-protection protocols ndpv6 culprit-flows fpc-slot 1
```

```
Currently tracked flows: 2, Total detected flows: 2
```


show ddos-protection protocols flow-detection

Syntax	<code>show ddos-protection protocols <protocol-group> flow-detection <brief detail terse></code>
Release Information	<p>Command introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	Display flow detection information for all protocol groups or for a particular protocol group.
Options	<p>none—Display information for all protocol groups.</p> <p>brief detail terse—(Optional) Display the specified level of output.</p> <ul style="list-style-type: none"> • brief—Display basic function information. • detail—Add information to the brief output; it is identical to the output displayed when you choose no option. The brief and detail options display information for all protocol groups, which can be a long list. • terse—Display the same level of information as the brief option but only for active protocol groups. <p>protocol-group—(Optional) Display information for a particular protocol group. See show ddos-protection protocols for a list of available groups.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear ddos-protection protocols on page 1077 • show ddos-protection protocols on page 1132 • show ddos-protection protocols culprit-flows on page 990 • show ddos-protection protocols parameters on page 1153 • show ddos-protection protocols statistics on page 1160 • show ddos-protection protocols violations on page 1171
List of Sample Output	<p>show ddos-protection protocols flow-detection on page 999</p> <p>show ddos-protection protocols flow-detection brief (Parameters for a Specific Protocol) on page 1000</p>

Output Fields Table 39 on page 998 lists the output fields for the **show ddos-protection protocols flow-detection** command. Output fields are listed in the approximate order in which they appear.

Table 39: show ddos-protection protocols flow-detection Output Fields

Field Name	Field Description	Level of Output
Packet types	Number of packet types.	All levels
Modified	Number of packets for which policer values have been modified from the default.	All levels
Protocol Group	Name of protocol group.	All levels
Packet type	Name of packet type in protocol group.	All levels
Flow detection configuration	Configuration of flow detection at the packet level.	detail none
Detection mode or Op mode	Mode of operation for flow detection at the packet level: <ul style="list-style-type: none"> • Automatic or a—Search flows only when a policer is being violated. • Off or x—Never search flows even when a policer is being violated. • On or o—Search flows even when no policer is being violated. 	All levels
Policer BW (pps)	Bandwidth allowed at the packet level.	brief terse
Detect time	Time in seconds that a suspicious flow that has exceeded the bandwidth allowed for the packet type must remain in violation to be confirmed as a culprit flow.	detail none
Log flows or Log flow	State of automatic logging of suspicious traffic flows for the packet type: on (Yes) or off (No).	All levels
Recover time	Time in seconds that must pass before a culprit flow for the packet type is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation.	detail none
Timeout flows or Time out	State of timeout enabling for culprit flows: <ul style="list-style-type: none"> • Yes—Enabled; flows can time out (released from suppression) when a timeout period expires, regardless of whether flow is still in violation. • No—Disabled; flows are not allowed to time out. 	All levels
Timeout time	Time in seconds that a culprit flow is suppressed. On expiration, the flow times out even if it is still violating the bandwidth limit.	detail none
Flow aggregation level configuration	Configuration of flow detection for each flow aggregation level.	detail none

Table 39: show ddos-protection protocols flow-detection Output Fields (continued)

Field Name	Field Description	Level of Output
Aggregation level or Agg level	One of three levels of flow aggregation <ul style="list-style-type: none"> • Subscriber or sub • Logical interface or ifl • Physical interface or ifd 	All levels
Detection mode or Op	Mode of operation for flow detection at the flow aggregation level: <ul style="list-style-type: none"> • Automatic—Search flows only when a policer is being violated. • Off—Never search flows even when a policer is being violated. • On—Search flows even when no policer is being violated. 	All levels
Control mode or Fc	Mode by which traffic in a culprit flow is handled. <ul style="list-style-type: none"> • drop—Drop all traffic in flow. • keep—Keep all traffic in flow. • police—Police the traffic to within its allowed bandwidth. 	All levels
Flow rate or BWidth (pps)	Bandwidth allowed at the flow aggregation level.	brief terse

Sample Output

show ddos-protection protocols flow-detection

```

user@host> show ddos-protection protocols flow-detection

Packet types: 190, Modified: 2
* = User configured value

Protocol Group: IPv4-Unclassified

  Packet type: aggregate
  Flow detection configuration:
    Detection mode: Automatic Detect time: 3 seconds
    Log flows:      No         Recover time: 60 seconds
    Timeout flows:  No         Timeout time: 300 seconds
  Flow aggregation level configuration:
    Aggregation level  Detection mode  Control mode  Flow rate
    Subscriber         Automatic     Drop          10 pps
    Logical interface   Automatic     Drop          10 pps
    Physical interface  Automatic     Drop          2000 pps

Protocol Group: IPv6-Unclassified

  Packet type: aggregate
  Flow detection configuration:
    Detection mode: Automatic Detect time: 3 seconds
    Log flows:      No         Recover time: 60 seconds
    Timeout flows:  No         Timeout time: 300 seconds
  Flow aggregation level configuration:
    Aggregation level  Detection mode  Control mode  Flow rate

```

Subscriber	Automatic	Drop	10 pps
Logical interface	Automatic	Drop	10 pps
Physical interface	Automatic	Drop	2000 pps

...

show ddos-protection protocols flow-detection brief (Parameters for a Specific Protocol)

```
user@host> show ddos-protection protocols dhcpv4 flow-detection brief
```

```
Packet types: 19, Modified: 1
```

```
* = User configured value
```


```
Detection mode(Op): a = automatic      Flow control mode(Fc): d = drop
                      o = on              k = keep
                      x = off             p = police
```

Protocol group	Packet type	Op mode	Policer BW(pps)	Aggr level sub	Op:Fc:BW(pps) ifl	Op:Fc:BW(pps) ifd	Log flow	Time out
dhcpv4	aggregate	auto	5000	a:d:10	a:d:10	a:d:5000	No	No
dhcpv4	unclass..	auto	300	a:d:10	a:d:10	a:d:300	No	No
dhcpv4	discover	auto	777*	a:d:10	a:d:10	a:d:500	No	No
dhcpv4	offer	auto	1000	a:d:10	a:d:10	a:d:1000	No	No
dhcpv4	request	auto	1000	a:d:10	a:d:10	a:d:1000	No	No
dhcpv4	decline	auto	500	a:d:10	a:d:10	a:d:500	No	No
dhcpv4	ack	auto	500	a:d:10	a:d:10	a:d:500	No	No
dhcpv4	nak	auto	500	a:d:10	a:d:10	a:d:500	No	No
dhcpv4	release	auto	2000	a:d:10	a:d:10	a:d:2000	No	No
dhcpv4	inform	auto	500	a:d:10	a:d:10	a:d:500	No	No
dhcpv4	renew	auto	2000	a:d:10	a:d:10	a:d:2000	No	No
dhcpv4	forcerenew	auto	2000	a:d:10	a:d:10	a:d:2000	No	No
dhcpv4	leasequery	auto	2000	a:d:10	a:d:10	a:d:2000	No	No
dhcpv4	leaseuna..	auto	2000	a:d:10	a:d:10	a:d:2000	No	No
dhcpv4	leaseunk..	auto	2000	a:d:10	a:d:10	a:d:2000	No	No
dhcpv4	leaseact..	auto	2000	a:d:10	a:d:10	a:d:2000	No	No
dhcpv4	bootp	auto	300	a:d:10	a:d:10	a:d:300	No	No
dhcpv4	no-msgtype	auto	0	a:d:10	a:d:10	a:d:0	No	No
dhcpv4	bad-pack..	auto	0	a:d:10	a:d:10	a:d:0	No	No

source-mac-address-list

Syntax	<code>source-mac-address-list <i>address-list-name</i>;</code>
Hierarchy Level	<p>[edit forwarding-options access-security router-advertisement-guard policy <i>policy-name</i> discard]</p> <p>[edit forwarding-options access-security router-advertisement-guard policy <i>policy-name</i> accept match-list]</p>
Release Information	<p>Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.</p> <p>Statement introduced in Junos OS Release 16.1 for EX Series switches.</p>
Description	<p>Configure a list of MAC addresses for an IPv6 Router Advertisement (RA) guard policy to validate the source MAC address of an incoming RA message against the MAC addresses in this list. RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in the policy.</p> <p>You can use a list of MAC address for validating RA messages as part of either an accept policy or a discard policy. Before you can include a list in an RA policy, you must configure the list name at the [edit policy-options mac-list] hierarchy level. When RA guard is enabled by using an accept policy, any RA messages that match the conditions defined in the policy are forwarded, and RA messages that do not match the conditions are dropped. When RA guard is enabled by using a discard policy, any RA messages that match the conditions are dropped, and RA messages that do not match the conditions are forwarded.</p>
Options	<i>address-list-name</i> —Configure the RA guard policy to match the MAC source address of an incoming RA message to a MAC address contained in the list.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514

spi (Junos OS)

Syntax	<code>spi spi-value;</code>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bi-directional)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the security parameter index (SPI) for a security association (SA).
Options	spi-value —An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet). Range: 256 through 16,639
<div> NOTE: Use the auxiliary SPI when you configure the protocol statement to use the bundle option.</div>	
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

spi (Junos-FIPS Software)

Syntax	<code>spi spi-value;</code>
Hierarchy Level	[edit security ipsec internal security-association manual direction]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	The security parameter index (SPI) value used for the internal Routing Engine-to-Routing Engine IPsec security association (SA) configuration.
Options	spi-value —Integer to use for this SPI. Range: 256 through 16,639
Required Privilege Level	Crypto Officer—To add and view this statement in the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 211• <i>Secure Configuration Guide for Common Criteria and Junos-FIPS</i>

ssh

Syntax	<pre>ssh { authentication-order [<i>method 1 method2...</i>]; ciphers [<i>cipher-1 cipher-2 cipher-3 ...</i>]; client-alive-count-max <i>seconds</i>; client-alive-interval <i>seconds</i>; connection-limit <i>limit</i>; fingerprint-hash (md5 sha2-256); hostkey-algorithm (<i>algorithm</i> <i>no-algorithm</i>); key-exchange [<i>algorithm1 algorithm2...</i>]; log-key-changes <i>log-key-changes</i>; macs [<i>algorithm1 algorithm2...</i>]; max-sessions-per-connection <<i>number</i>>; no-passwords; no-public-keys; no-tcp-forwarding; protocol-version [v2]; rate-limit <i>limit</i>; root-login (allow deny deny-password); sftp-server; } tcp-forwarding (JDM)</pre>
Hierarchy Level	[edit system services]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>client-alive-interval and client-alive-max-count statements introduced in Junos OS Release 12.2.</p> <p>no-passwords statement introduced in Junos OS Release 13.3.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>no-public-keys statement introduced in Junos OS release 15.1.</p> <p>tcp-forwarding statement introduced in Junos OS Release 15.1X53-D50 for the NFX250 Network Services Platform.</p> <p>fingerprint-hash statement introduced in Junos OS Release 16.1.</p> <p>log-key-changes statement introduced in Junos OS Release 17.4R1.</p> <p>sftp-server statement introduced in Junos OS Release 19.1R1.</p>
Description	<p>Allow SSH requests from remote systems to access the local router or switch.</p> <p>The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- *Configuring SSH Service for Remote Access to the Router or Switch*

ssh-known-hosts

Syntax

```
ssh-known-hosts {
  fetch-from-server server;
  host hostname {
    dsa-key key;
    ecdsa-sha2-nistp256-key key;
    ecdsa-sha2-nistp384-key key;
    ecdsa-sha2-nistp521-key key;
    ed25519-key key;
    rsa-key key;
    rsa1-key key;
  }
  load-key-file filename;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 7.5.

Description Configure SSH support for known hosts and for administering SSH host key updates.

Options **fetch-from-server *server***—Retrieve SSH public host key information from the specified server. Specify by server name or IP address.

host *host-name*—Hostname of the SSH known host entry. This option has the following suboptions:

- **dsa-key *key***—Base64 encoded Digital Signature Algorithm (DSA) key for SSH version 2.
- **ecdsa-sha2-nistp256-key *key***—Base64 encoded ECDSA-SHA2-NIST256 key.
- **ecdsa-sha2-nistp384-key *key***—Base64 encoded ECDSA-SHA2-NIST384 key.
- **ecdsa-sha2-nistp521-key *key***—Base64 encoded ECDSA-SHA2-NIST521 key.
- **ed25519-key *key***—Base64 encoded ED25519 key.
- **rsa-key *key***—Base64 encoded public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.
- **rsa1-key *key***—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.

load-key-file *filename*—Import SSH host key information from the named file. If the file is in a directory other than the home directory of the device, specify pathname as well.

Required Privilege	admin—To view this statement in the configuration.
Level	admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring SSH Host Keys for Secure Copying of Data</i>

start-time (Authentication Key Transmission)

Syntax	<code>start-time (now yyyy-mm-dd.hh:mm:ss);</code>
Hierarchy Level	<code>[edit security authentication-key-chains key-chain <i>key-chain-name</i> key <i>key</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 11.3 for QFX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Specify a start time for key transmission. You do not need to specify an end time for the key. If a new key is present with a new start time, the keychain rolls over to the new one. The start time must be unique within the keychain.</p>
Options	<p>now—Start time as the current year, month, day, hour, minute, and second.</p> <p>daydays—Start time as the specified number of days after the current day. For example, if the current day is the 12th and you configure start-time 2day, the start time will be on the 14th, exactly two days after the configuration is entered.</p> <p>hourhours—Start time as the specified number of hours after the current hour. For example, if the current hour is 9:00 and you configure start-time 3hour, the start time will be in 12:00, exactly three hours after the configuration is entered.</p> <p>minuteminutes—Start time as the specified number of minutes after the current minute. For example, if the current minute is 27 minutes after the hour and you configure start-time 5min, the start time will be in 32 minutes after the hour, exactly five minutes after the configuration is entered.</p> <p>monthmonths—Start time as the specified number of months after the current month. For example, if the current month is March and you configure start-time 4month, the start time will be in July, exactly four months after the configuration is entered.</p> <p>secondseconds—Start time as the specified number of seconds after the current second. For example, if the current second is 10:20:40 and you configure start-time 10seconds, the start time will be 10:20:50, exactly 10 seconds after the configuration is entered.</p> <p>yearyears—Start time as the specified number of years after the current year. For example, if the current year is 2011 and you configure start-time 1year, the start time will be in 2012, exactly one year after the configuration is entered.</p> <p>yyyy-mm-dd.hh:mm:ss—Start time in UTC (Coordinated Universal Time). The start time must be unique within the keychain.</p>

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols</i>• <i>Example: Configuring BFD Authentication for Securing Static Routes</i>• <i>Example: Configuring BFD Authentication for Securing Static Routes</i>• <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

stateful

Syntax	(stateful stateless);
Hierarchy Level	[edit forwarding-options access-security router-advertisement-guard interface (interface-name interface-range-name)] [edit forwarding-options access-security router-advertisement-guard vlans vlan-name]
Release Information	Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Statement introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Configure stateful IPv6 Router Advertisement (RA) guard. In an IPv6 deployment, RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. RA guard performs checks on incoming RA messages to make sure that they are sent from legitimate routers. If the sender of the RA message cannot be validated, the RA message is dropped.</p> <p>Stateful RA guard enables the switch to learn about the sources of RA messages for a certain period of time. During this period, when the switch is known to be in the learning state, the information contained in attributes of received RA messages is stored and compared to the policy. When the learning period ends, the switch has a record of which interfaces are attached to links with valid IPv6 routers. If there is no valid IPv6 router attached to the interface, the switch dynamically transitions the interface from the learning state into the blocking state. Subsequent RA messages received after the transition to blocking state are dropped. If there is a valid IPv6 router attached to the interface, the interface transitions to the forwarding state, and subsequent RA messages that can be validated against the configured policy are forwarded.</p> <p>You can enable stateful RA guard on an interface or on a VLAN. When you enable stateful RA guard, the initial state is Off. You initiate the learning state by issuing the request access-security router-advertisement-guard-learn command.</p>
Default	RA guard is stateless by default.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Stateless IPv6 Router Advertisement Guard on page 517 Configuring Stateful IPv6 Router Advertisement Guard on page 514

stateless

Syntax	(stateful stateless);
Hierarchy Level	[edit forwarding-options access-security router-advertisement-guard interface (interface-name interface-range-name)] [edit forwarding-options access-security router-advertisement-guard vlans vlan-name]
Release Information	Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Statement introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Configure stateless IPv6 Router Advertisement (RA) guard. In an IPv6 deployment, RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in a policy.</p> <p>You can configure RA guard to be stateless or stateful. If stateless RA guard is enabled, the switch examines incoming RA messages and filters each message on the basis of whether it matches the conditions configured in the policy. After the switch has validated the content of the RA message, it forwards the RA message to its destination; otherwise, the RA message is dropped. For example, an interface can be statically configured to forward RA messages only from predefined sources.</p> <p>You can enable stateless RA guard on an interface or on a VLAN.</p>
Default	RA guard is stateless by default.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514

static-ip

Syntax

```
static-ip ip-addresses {
  vlan vlan-name;
  mac mac-address;
}
```

Hierarchy Level

- For platforms with ELS:

```
[edit vlans vlan-name forwarding-options dhcp-security group group-name interface
 interface-name]
```

- For platforms without ELS:

```
[edit ethernet-switching-options secure-access-port interface (all | interface-name)]
```

Release Information Statement introduced in Junos OS Release 9.2 for EX Series switches. Hierarchy level `[edit vlans vlan-name forwarding-options dhcp-security]` introduced in Junos OS Release 13.2X50-D10. (See *Using the Enhanced Layer 2 Software CLI* for information about ELS.)

Description Configure a static IP address to MAC address (IP-MAC) binding to be added to the DHCP snooping database.



NOTE: The VLAN is specified at the higher hierarchy level when `static-ip` is configured at `[edit vlans vlan-name forwarding-options dhcp-security group group-name interface interface-name]`.

Options `ip-address`—Static IP address assigned to a device connected on the specified interface.

`mac mac-address`—Static MAC address assigned to a device connected on the specified interface.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level `system`—To view this statement in the configuration.
`system-control`—To add this statement to the configuration.

Related Documentation

- [Configuring Static DHCP IP Addresses for DHCP snooping \(non-ELS\) on page 405](#)
- [Configuring Static DHCP IP Addresses for DHCP snooping \(ELS\) on page 404](#)

static-ip (MX Series)

Syntax	<code>static-ip <i>ip-address</i> mac <i>mac-address</i>;</code>
Hierarchy Level	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security group <i>group-name</i> interface <i>interface-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	Configure a static IP address to MAC address (IP-MAC) binding record to be added to the DHCP snooping database.
Options	<p><i>ip-address</i>—Static IP address assigned to a device connected on the specified interface.</p> <p><i>mac-address</i>—Static MAC address assigned to a device connected on the specified interface.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static DHCP IP Addresses for DHCP snooping (MX routers) on page 406

static-ipv6

Syntax	<pre>static-ipv6 ip-address { mac mac-address; }</pre>
Hierarchy Level	<pre>[edit vlans vlan-name forwarding-options dhcp-security group group-name interface interface-name]; [edit ethernet-switching-options secure-access-port interface interface-name]</pre>
Release Information	Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches. Support at the <code>[edit ethernet-switching-options secure-access-port interface interface-name]</code> hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Configure a static IP-MAC binding to be added to the DHCPv6 snooping database.
Options	<p>ip-address—Static IPv6 address assigned to a device connected on the specified interface.</p> <p>mac mac-address—Static MAC address assigned to a device connected on the specified interface.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Static DHCP IP Addresses for DHCP snooping (ELS) on page 404

storm-control

Syntax

```
storm-control {
  action-shutdown;
  interface (all | interface-name) {
    bandwidth bandwidth;
    level level;
    multicast;
    no-broadcast;
    no-multicast;
    no-registered-multicast;
    no-unknown-unicast;
    no-unregistered-multicast;
  }
}
```

Hierarchy Level [edit [ethernet-switching-options](#)]

Release Information Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure storm control on the switch.


The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Autorecovery for Port Security Events on page 635](#)
- [Understanding Storm Control on page 622](#)

storm-control

Syntax	<code>storm-control storm-control-profile;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>number</i> family ethernet-switching], [edit interfaces <i>interface-name</i> unit <i>number</i> family bridge] [edit interfaces <i>interface-name</i> ether-options ethernet-switch-profile] [edit logical-systems <i>name</i> interfaces <i>interface-name</i> unit <i>number</i> family bridge]
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX series. Statement introduced in Junos OS Release 14.1 for the MX Series routers. Starting in Junos OS release 17.4R1 for MX Series routers, support for storm control was added for logical systems.
Description	<p>Bind a storm control profile to a given interface.</p> <p>On switches running ELS software, storm control is enabled by default on all switch interfaces at a level of 80 percent of the combined broadcast and unknown unicast streams. (For the equivalent statement for platforms running non-ELS software, see storm-control.)</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> NOTE: If you configure storm control on an aggregated Ethernet interface, the storm-control level is applied to each member interface individually. For example, if the aggregated interface has two members and you configure a storm-control level of 20 kbps, Junos will not detect a storm if one or both of the member interfaces receives traffic at 15 kbps because in neither of these cases does an individual member receive traffic at a rate greater than the configured storm-control level. In this example, Junos detects a storm only if at least one member interface receives traffic at greater than 20 Kbps.</p> </div>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches • Understanding Storm Control on page 622

storm-control

Syntax	<pre>storm-control { action-shutdown; interface (all <i>interface-name</i>) { bandwidth <i>bandwidth</i>; no-broadcast; no-multicast; no-unknown-unicast; } }</pre>
Hierarchy Level	[edit ethernet-switching-options]
Release Information	Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	<p>Apply storm control to all interfaces or to the specified interfaces on switches running non-ELS software. (For the equivalent statement for switches running ELS software, see storm-control.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Default	<p>On switches running non-ELS software, storm control is disabled by default on all switch interfaces. If you enable storm control and do not specify a storm control level, the default level is 80 percent of the available bandwidth for ingress traffic. You can change the storm control level by configuring it as a specific bandwidth value.</p> <p>When you configure storm control bandwidth on an aggregated Ethernet interface, each member of the aggregated interface is assigned that bandwidth. For example, if you configure 7000000 Kbps on aggregated interface ae1, and ae1 has two members, xe-2:0/0/0 and xe-2:0/0/1, each member is allowed a bandwidth level of 7000000 Kbps. Thus, the storm control bandwidth on ae1 could be as much as 14000000 Kbps of combined broadcast and unknown unicast traffic.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Storm Control on page 622 • Example: Using Storm Control to Prevent Network Outages (non-ELS) on page 638 • port-error-disable • disable-timeout on page 743 • clear ethernet-switching port-error

storm-control-profiles

Syntax

```
storm-control-profiles profile-name {
  action-shutdown;
  all {
    bandwidth-level;
    bandwidth-percentage;
    no-broadcast;
    no-multicast;
    no-registered-multicast;
    no-unknown-unicast;
    no-unregistered-multicast;
  }
}
```

Hierarchy Level

```
[edit forwarding-options]
[edit logical-systems name forwarding-options]
```

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
 Statement introduced in Junos OS Release 13.2 for the QFX Series.
 Statement introduced in Junos OS Release 14.1 for MX Series routers.
 Starting in Junos OS release 17.4R1 for MX Series routers, support for storm control was added for logical systems.

Description

Configure a storm control profile on a switch or router. Storm control is used to prevent network outages that are caused by broadcast traffic storms. Storm control enables the switching device to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the storm control level or storm control bandwidth—is exceeded, thus preventing packets from proliferating and degrading the LAN.



NOTE: The name of the storm control profile can contain no more than 127 characters.

The remaining statements are explained separately. See [CLI Explorer](#).


Required Privilege Level

system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- [Understanding Storm Control on page 622](#)

subscriber (DDoS Flow Detection)

Syntax	<code>subscriber (flow-bandwidth flow-control-mode flow-detection-mode)</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers. Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure flow bandwidth, flow control mode, or flow detection mode at the subscriber flow aggregation level for the packet type.
Options	<p>flow-bandwidth—Specify the bandwidth for the flow at the subscriber level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth] hierarchy level.</p> <p>Default: 100 packets per second</p> <p>Range: 1 through 10,000 packets per second</p> <p>flow-control-mode—Specify how traffic in the detected flow is controlled at the subscriber level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control] hierarchy level.</p> <hr/> <div>  <p>NOTE: The configuration at this level overrides the global configuration using the flow-level-control statement at the [edit system ddos-protection global] hierarchy level.</p> </div> <hr/> <ul style="list-style-type: none"> drop—Drop all traffic in flow. keep—Keep all traffic in flow. police—Police the traffic to within its allowed bandwidth. <p>Default: drop</p> <p>flow-detection-mode—Specify how flow detection operates at the subscriber level when a policer has been violated. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection] hierarchy level.</p>



NOTE: The configuration at this level overrides the global configuration using the `flow-detection-mode` statement at the `[edit system ddos-protection global]` hierarchy level.

- **automatic**—Search flows at the subscriber level only when a DDoS policer is being violated and only until it is established that the flow causing the violation is not at this level. When the suspicious flow is not at this level, then the search moves to a coarser level of flow aggregation (logical interface). Flows at the subscriber level are subsequently not searched again until the policer is no longer violated at the coarser level.
- **off**—Disable flow detection at the subscriber level so that flows are never searched at this level.
- **on**—Search flows at the subscriber level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

Default: `automatic`

Required Privilege Level	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 575• Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 572• Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 571• Configuring Flow Detection for DDoS Protection
------------------------------	--

switch-options (VLANs)

List of Syntax [Syntax \(EX Series, MX Series, QFX Series and NFX Series\) on page 1021](#)
[Syntax \(SRX Series\) on page 1021](#)

Syntax (EX Series, MX Series, QFX Series and NFX Series)

```
switch-options {
  interface interface-name {
    interface-mac-limit limit {
      packet-action drop;
    }
    mac-pinning
    no-mac-learning;
    static-mac static-mac-address {
      vlan-id number;
    }
  }
  interface-mac-limit limit {
    packet-action drop;
  }
  mac-statistics;
  mac-ip-table-size number;
  mac-table-size limit {
    packet-action drop;
  }
  no-mac-learning;
  service-id number;
  vtep-source-interface
}
```

Syntax (SRX Series)

```
switch-options {
  interface interface-name {
    encapsulation-type;
    ignore-encapsulation-mismatch;
    pseudowire-status-tlv;
    static-mac mac-address {
      vlan-id vlan-id;
    }
  }
  mac-table-aging-time seconds;
  mac-table-size {
    number;
    packet-action drop;
  }
}
```

EX Series, MX Series, QFX Series and NFX Series

```
[edit ],
[edit logical-systems logical-system-name routing-instances routing-instance-name vlans
  vlan-name],
[edit routing-instances routing-instance-name vlans vlan-name],
[edit vlans vlan-name]
```

SRX Series	[edit vlans <i>vlans-name</i>]
Release Information	<p>Statement modified in Junos OS Release 9.5.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches and MX Series routers.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement (mac-pinning) introduced in Junos OS 16.2 for MX Series routers.</p> <p>mac-ip-table-size statement introduced in Junos OS 17.4 Release for MX Series routers and EX9200 switches.</p>
Description	<p>Configure Layer 2 learning and forwarding properties for a VLAN or a virtual switch.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Ethernet Switching and Layer 2 Transparent Mode Overview</i>

timeout

Syntax	<code>timeout <i>seconds</i>;</code>
Hierarchy Level	<code>[edit ethernet-switching-options secure-access-port dhcp-snooping-file];</code> <code>[edit ethernet-switching-options secure-access-port dhcpv6-snooping-file]</code>
Release Information	Statement introduced in Junos OS Release 9.4 for EX Series switches. Support at the <code>[edit ethernet-switching-options secure-access-port dhcpv6-snooping-file]</code> hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Specify a timeout value for remote read and write operations. This value determines the amount of time that the switch waits for a remote system to respond when the DHCP snooping database is stored on the remote FTP site.
Default	None
Options	<i>seconds</i> —Value in seconds. Range: 10 through 3600.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Persistent Bindings in the DHCP or DHCPv6 (non-ELS) on page 383 • Understanding DHCP Snooping (non-ELS) on page 393

timeout-active-flows (DDoS Flow Detection)

Syntax	timeout-active-flows;
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i>]
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Enable culprit flows for the packet type to time out according to the timeout period. The culprit flow is suppressed for the duration of the timeout period. When the period expires, the flow times out and is released from suppression.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Timeout Period for a Culprit Flow on page 570• <i>Configuring Flow Detection for DDoS Protection</i>

tolerance

Syntax	<code>tolerance seconds;</code>
Hierarchy Level	<code>[edit security authentication-key-chains key-chain <i>key-chain-name</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in Junos OS Release 11.2.</p>
Description	Configure the clock-skew tolerance for accepting keys for a key chain.
Options	<p>seconds—Number of seconds to accept for clock-skew.</p> <p>Default: 0 seconds</p> <p>Range: 0 through 4294967295 seconds</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols</i> • <i>Example: Configuring BFD Authentication for Securing Static Routes</i> • <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

traceoptions

Syntax

```

traceoptions {
  file filename <files number> <size size>;
  flag all;
  flag certificates;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
  level
  no-remote-trace
}

```

Hierarchy Level [edit security],
[edit services ipsec-vpn]

Trace options can be configured at either the [edit security] or the [edit services ipsec-vpn] hierarchy level, but not at both levels.

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure security trace options.

To specify more than one trace option, include multiple **flag** statements. Trace option output is recorded in the `/var/log/kmd` file.



NOTE: The `traceoptions` statement is not supported on QFabric systems.

Options **files *number***—(Optional) Maximum number of trace files. When a trace file (for example, `kmd`) reaches its maximum size, it is renamed `kmd.0`, then `kmd.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the **size** option.

Range: 2 through 1000 files

Default: 0 files

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, **kmd**) reaches this size, it is renamed, **kmd.0**, then **kmd.1** and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Default: 1024 KB

flag *flag*—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all security events.
- **certificates**—Trace certificate events.
- **database**—Trace database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **timer**—Trace internal timer events.

level *level*—(Optional) Set traceoptions level.

- **all**—match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing

Required Privilege	admin—To view the configuration.
Level	admin-control—To add this statement to the configuration.

Related Documentation	• Configuring Tracing Operations on page 203
------------------------------	--

traceoptions (Access Port Security)

Syntax	<pre> traceoptions { file (<i>file-name</i> files <i>files</i> match <i>match</i> no-world-readable size <i>size</i> world-readable); flag (all asynch chassis-scheduler cos-adjustment dynamic hardware-database init parse performance-monitor process restart route-socket show snmp util); no-remote-trace; } </pre>
Hierarchy Level	[edit ethernet-switching-options], [edit class-of-service]
Release Information	Statement introduced in Junos OS Release 9.2 for EX Series switches.
Description	Define global tracing operations for access security features on Ethernet switches.
Default	The traceoptions feature is disabled by default.
Options	<p>disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.</p> <p>file <i>filename</i>—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.</p> <p>files <i>number</i>—(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 (xk to specify KB, xm to specify MB, or xg to specify gigabytes), at which point the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • access-security—Trace access security events. • all—All tracing operations. • config-internals—Trace internal configuration operations. • forwarding-database—Trace forwarding database and next-hop events. • general—Trace general events. • interface—Trace interface events.

- **ip-source-guard**—Trace IP source guard events.
- **krt**—Trace communications over routing sockets.
- **lib**—Trace library calls.
- **normal**—Trace normal events.
- **parse**—Trace reading of the configuration.
- **regex-parse**—Trace regular-expression parsing operations.
- **rtg**—Trace redundant trunk group events.
- **state**—Trace state transitions.
- **stp**—Trace spanning-tree events.
- **task**—Trace Ethernet-switching task processing.
- **timer**—Trace Ethernet-switching timer processing.
- **vlan**—Trace VLAN events.

no-stamp—(Optional) Do not timestamp the trace file.

Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Restrict file access to the user who created the file.

replace—(Optional) Replace an existing trace file if there is one rather than appending to it.

Default: If you do not include this option, tracing output is appended to an existing trace file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes. 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. If you specify a maximum number of files, you also must specify a maximum file size with the **files** option.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify gigabytes

Range: 10 KB through 1 gigabyte

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

no-remote-trace—(Optional) Disable remote tracing.

Required Privilege Level	system—To view this statement in the configuration.
	system-control—To add this statement to the configuration.

- Related Documentation**
- [Port Security Features on page 3](#)
 - *Interfaces Overview for Switches*
 - [Understanding IP Source Guard for Port Security on Switches on page 459](#)
 - *Understanding Redundant Trunk Links (Legacy RTG Configuration)*
 - *Understanding STP*
 - *Understanding Bridging and VLANs on Switches*

traceoptions (DDoS)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; } </pre>
Hierarchy Level	[edit system ddos-protection]
Release Information	<p>Statement introduced in Junos OS Release 11.2 for MX Series routers with MPCs.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches, and T4000 routers with FPC5s.</p> <p>Statement introduced in Junos OS Release 14.1X53 on QFX Series switches.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	Define tracing operations for DDoS protection processes.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • all—Trace all operations. • config—Trace processing of the DDoS configuration at an extensive level. • events—Trace jddosd event processing; currently only exit events are traced. • gres—Trace messages exchanged with the kernel and jddosd process that could affect graceful Routing Engine switchover (GRES). • init—Trace jddosd initialization. • ipc—Trace interface interprocess communication (IPC) messages. • memory—Trace memory management code. This flag is not currently supported. • protocol—Trace DDoS protocol state processing. Only the violation state is currently traced. • rtsock—Trace messages exchanged with the kernel and jddosd process.

- **signal**—Trace system signals that are passed to jddosd, such as SIGTERM.
- **socket**—Trace socket messages that are passed to jddosd from the Packet Forwarding Engine.
- **state**—Trace state machine events. This flag is not currently supported.
- **timer**—Trace jddosd timer events.
- **ui**—Trace user interface processing. This flag is not currently supported.

level—Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.


Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10,240 through 1,073,741,824

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Tracing DDoS Protection Operations on page 543

traceoptions (DHCP)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; } </pre>
Hierarchy Level	<p>[edit system processes dhcp-service] [edit security dynamic-address]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.1 for EX Series switches. Statement introduced in Junos OS Release 18.4R1.</p>
Description	<p>Define global tracing operations for extended DHCP local server and extended DHCP relay agent processes.</p> <p>This statement replaces the deprecated traceoptions statements at the [edit forwarding-options dhcp-relay] and [edit system services dhcp-local-server] hierarchy levels.</p>
<div style="display: flex; align-items: center;">  <div> <p>NOTE: Traceoptions does not differentiate between a logical system and tenant system, and can be configured under the root logical system.</p> </div> </div>	
Options	<p>file <i>filename</i>—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.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000 Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements:</p> <ul style="list-style-type: none"> • all—Trace all events. • auth—Trace authentication events. • database—Trace database events. • fwd—Trace firewall process events.

- **general**—Trace miscellaneous events.
- **ha**—Trace high availability-related events.
- **interface**—Trace interface operations.
- **io**—Trace I/O operations.
- **liveness-detection**—Trace liveness detection operations.
- **packet**—Trace packet and option decoding operations.
- **performance**—Trace performance measurement operations.
- **profile**—Trace profile operations.
- **rpd**—Trace routing protocol process events.
- **rtsock**—Trace routing socket operations.
- **security-persistence**—Trace security persistence events.
- **session-db**—Trace session database events.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

level—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

Default: **error**

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access, allowing only the user **root** and users who have the Junos OS **maintenance** permission to access the trace files.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (*maximum-file-sizek*), megabytes (*maximum-file-sizem*), or gigabytes (*maximum-file-sizeg*). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Range: 10,240 through 1,073,741,824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• <i>Tracing Extended DHCP Operations</i>
------------------------------	---

traceoptions (MACsec)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } </pre>
Hierarchy Level	[edit security macsec]
Release Information	<p>Statement introduced in Junos OS Release 15.1 for MIC-3D-20GE-SFP-E on MX Series routers.</p> <p>Statement introduced in Junos OS Release 16.1 for MPC7E-10G on MX Series routers.</p> <p>Statement introduced in Junos OS Release 17.3R2 for JNP-MIC1-MACSEC MIC on MX10003 routers.</p>
Description	<p>Define tracing operations at the MACsec level. Tracing operations provide support for debugging protocol-level issues. MACsec is an industry-standard security technology that provides secure communication for almost all types of traffic on Ethernet links. To specify more than one tracing operation, include multiple flag statements.</p> <p>The interfaces traceoptions statement does not support a separate trace file. The logging is done by the kernel, so the tracing information is placed in the syslog file in the directory /var/log/dcd.</p>
Default	If you do not include this statement, no tracing operations are performed.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. By default, interface process tracing output is placed in the directory. If you do not specify the name of the trace file, all files are placed in the directory /var/log/dcd.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches the maximum value, 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. Values range from 2 through 1000.</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. The following are the tracing operation options:</p> <p>all—Trace all operations.</p> <p>config—Trace configuration messages.</p> <p>debug—Trace debug messages.</p> <p>normal—Trace normal messages.</p>

no-world-readable—(Optional) Prevent any user from reading the log file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

world-readable—(Optional) Allow any user to read the log file.

Required Privilege Level	admin—To view this statement in the configuration.
	admin-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• <i>Understanding Media Access Control Security (MACsec) on MX Series Routers</i>• Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268
------------------------------	--

traceoptions (MACsec interfaces)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } </pre>
Hierarchy Level	[edit security macsec interfaces <i>interface-name</i>]
Release Information	<p>Statement introduced in Junos OS Release 16.1 for MPC7E-10G on MX Series routers.</p> <p>Statement introduced in Junos OS Release 17.3R2 for JNP-MIC1-MACSEC MIC on MX10003 routers.</p>
Description	<p>Define tracing operations for individual MACsec interfaces. Tracing operations provide support for debugging protocol-level issues. MACsec is an industry-standard security technology that provides secure communication for almost all types of traffic on Ethernet links. To specify more than one tracing operation, include multiple flag statements.</p> <p>The interfaces traceoptions statement does not support a separate trace file. The logging is done by the kernel, so the tracing information is placed in the system syslog file in the directory /var/log/dcd.</p>
Default	If you do not include this statement, no tracing operations are performed.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. By default, interface process tracing output is placed in the directory. If you do not specify the name of the tracefile, all files are placed in the directory /var/log/dcd.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches the maximum value, 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. Values range from 2 through 1000.</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. The following are the tracing operation options:</p> <p>all—Trace all operations.</p> <p>keys—Trace key creation or generation information.</p> <p>mka-packets—Trace MACsec Key Agreement (MKA) protocol input and output packet information.</p> <p>normal—Trace all normal events and messages.</p> <p>state—Trace MKA protocol state information.</p>

to-secy—Trace MKA to security entity state change information.

no-world-readable—(Optional) Prevent any user from reading the log file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

world-readable—(Optional) Allow any user to read the log file.

Required Privilege Level	admin—To view this statement in the configuration.
	admin-control—To add this statement to the configuration.

Related Documentation	• <i>Understanding Media Access Control Security (MACsec) on MX Series Routers</i>
	• Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

transmit-interval (MACsec)

Syntax	<code>transmit-interval <i>interval</i>;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> mka]</code>
Release Information	Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	<p>Specifies the transmit interval for MACsec Key Agreement (MKA) protocol data units (PDUs).</p> <p>The MKA transmit interval setting sets the frequency for how often the MKA PDU is sent to the directly connected device to maintain MACsec on a point-to-point Ethernet link. A lower <i>interval</i> increases bandwidth overhead on the link; a higher <i>interval</i> optimizes the MKA protocol data unit exchange process.</p> <p>The transmit interval settings must be identical on both ends of the link when MACsec using static connectivity association key (CAK) security mode is enabled.</p> <p>We recommend increasing the interval to 6000 ms in high-traffic load environments.</p>
Default	The default transmit interval is 2000 milliseconds.
Options	<i>interval</i> —Specifies the transmit interval, in milliseconds.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring MACsec on EX, SRX and Fusion Devices on page 228

transmit-interval (MACsec for MX Series)

Syntax	<code>transmit-interval <i>interval</i>;</code>
Hierarchy Level	<code>[edit security macsec connectivity-association <i>connectivity-association-name</i> mka]</code>
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specifies the transmit interval for MACsec Key Agreement (MKA) protocol data units (PDUs).</p> <p>The MKA transmit interval setting sets the frequency for how often the MKA PDU is sent to the directly connected device to maintain MACsec on a point-to-point Ethernet link. A lower <i>interval</i> increases bandwidth overhead on the link; a higher <i>interval</i> optimizes the MKA protocol data unit exchange process.</p> <p>The transmit interval settings must be identical on both ends of the link when MACsec using static connectivity association key (CAK) security mode is enabled.</p> <p>We recommend increasing the interval to 6000 milliseconds in high-traffic and large scale configuration load environments.</p>
Default	The default transmit interval is 2000 milliseconds.
Options	<i>interval</i> —Specifies the transmit interval, in milliseconds.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

trusted

Syntax	trusted;
Hierarchy Level	[edit bridge domains <i>bridge-domain-name</i> forwarding-options dhcp-security group <i>group-name</i> overrides]
Release Information	Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	Allow DHCP responses from the specified interface.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling a Trusted DHCP Server (MX Series Routers) on page 373 • <i>OBSOLETE: Understanding Trusted DHCP Servers for Port Security</i>

trusted (DHCP Security)

Syntax	trusted;
Hierarchy Level	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security group <i>group-name</i> overrides]
Release Information	Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX series.
Description	Specify that the interface in this group is trusted. DHCP snooping and DHCPv6 snooping do not apply to the trusted interface, even if the VLAN is enabled for DHCP or DHCPv6 snooping. Likewise, DAI, IP source guard, IPv6 source guard, and IPv6 neighbor discovery inspection—even if they are enabled for the VLAN—do not apply to the interface that is configured with the overrides and the trusted options. Access interfaces are untrusted by default.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling a Trusted DHCP Server (ELS) on page 372 • <i>OBSOLETE: Understanding Trusted DHCP Servers for Port Security</i> • Understanding DHCP Snooping (non-ELS) on page 393

unknown-unicast-forwarding

Syntax

```
unknown-unicast-forwarding {
  vlan vlan-name {
    interface interface-name;
  }
}
```

Hierarchy Level

- For platforms with ELS:

[edit switch-options]

- For platforms without ELS:

[edit ethernet-switching-options]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
 Statement introduced in Junos OS Release 13.2 for the QFX Series.
 Hierarchy level [edit switch-options] introduced in Junos OS Release 13.2X50-D10. (See *Using the Enhanced Layer 2 Software CLI* for information about ELS.)
 Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the switch to forward all unknown unicast packets in a VLAN or on all VLANs to a particular interface.



NOTE: Before you can configure unknown unicast forwarding within a VLAN, you must first configure that VLAN.

The remaining statements are explained separately. See [CLI Explorer](#).

Default

Unknown unicast packets are flooded to all interfaces that belong to the same VLAN.


Required Privilege Level

system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- [show vlans](#)
- [show ethernet-switching table on page 1198](#)
- [Understanding and Preventing Unknown Unicast Forwarding on page 613](#)

untrusted

Syntax	<code>untrusted;</code>
Hierarchy Level	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security group <i>group-name</i> overrides]</code>
Release Information	Statement introduced in Junos OS Release 13.2 for EX Series switches.
Description	<p>Configure a trunk interface as untrusted for DHCP security. Trunk interfaces are trusted by default and all packets are allowed. You can override this default behavior and set a trunk interface as untrusted in order to support DHCP security features on the interface. DHCP snooping, DHCPv6 snooping, dynamic ARP inspection (DAI), and IPv6 neighbor discovery inspection are supported on trunk ports in untrusted mode.</p> <p> NOTE: IP source guard and IPv6 source guard are not supported on untrusted trunk ports.</p> <p>Configuring a trunk port as untrusted is useful in deployments where multiple DHCP clients are aggregated onto one interface on the access device. In this scenario, the interface is configured as a trunk interface with one or more VLANs. A DHCP client attached to a trunk interface might start acting as a DHCP server. Trusted ports allow DHCP servers to provide IP addresses and other information to requesting devices, which makes the network vulnerable to a rogue DHCP server attack.</p> <p>An unauthorized DHCP server might also assign itself as the default gateway device for the network. An attacker can then sniff the network traffic and perpetrate a man-in-the-middle attack—that is, it misdirects traffic intended for a legitimate network device to a device of its choice. To mitigate this problem, you can configure the interface to which the unauthorized server is connected as untrusted, which blocks all ingress DHCP server messages from that interface.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding and Using Trusted DHCP Servers on page 371 • Configuring a Trunk Interface as Untrusted for DHCP Security (CLI Procedure)

untrusted

Syntax	untrusted;
Hierarchy Level	[edit bridge domains <i>bridge-domain-name</i> forwarding-options dhcp-security group <i>group-name overrides</i>]
Release Information	Statement introduced in Junos OS Release 14.1 for the MX Series.
Description	Allow DHCP responses from the specified interface.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling a Trusted DHCP Server (MX Series Routers) on page 373• <i>OBSOLETE: Understanding Trusted DHCP Servers for Port Security</i>

url (Security)

Syntax	url <i>url-name</i> ;
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i> enrollment], [edit security pki ca-profile <i>ca-profile-name</i> revocation-check <i>crl</i>]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	(Supported on Adaptive Services (AS) and MultiServices PICs only.) Specify the certificate authority (CA) URL to use in requesting digital certificates or the URL for the Lightweight Directory Access Protocol (LDAP) location from which the certificate revocation list (CRL) is retrieved.
Options	<p>url-name—Location of the CA to which enrollment requests are sent or LDAP location of the CRL. With Simple Certificate Enrollment Protocol (SCEP), you enroll CA certificates with the request security pki ca-certificate enroll command and specify the CA profile. There is no separate command to enroll CA certificates with CMPv2.</p> <p>The format of the URL is protocol http.</p>
Required Privilege Level	admin—To view the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying an Enrollment URL on page 187• Specifying an LDAP URL on page 188• crl on page 713

use-interface-description

Syntax	<code>use-interface-description (device logical);</code>
For Platforms with Enhanced Layer 2 Software (ELS)	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 circuit-id]</code>
For Platforms Without ELS	<code>[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>) dhcp-option82 circuit-id],</code> <code>[edit forwarding-options helpers bootp dhcp-option82 circuit-id],</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82 circuit-id],</code> <code>[edit ethernet-switching-options secure-access-port vlan (all <i>vlan-name</i>) dhcp-option82 remote-id],</code> <code>[edit forwarding-options helpers bootp dhcp-option82 remote-id],</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82 remote-id]</code>
For MX Series Platforms	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82circuit-id]</code>
Release Information	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Hierarchy level <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Hierarchy level <code>[edit bridge-domains <i>bridge domain name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.</p>
Description	<p>Use the interface description rather than the interface name (which is the default value) in the circuit ID or remote ID value in the DHCP option 82 information.</p> <p>The textual description is configured using the description statement at the <code>[edit interfaces <i>interface-name</i>]</code> hierarchy level. If you specify that the textual description be used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name. When you use the interface description rather than the interface name, the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.</p>
Options	<p>device—Use the device interface description. Only available for MX Series platform configuration.</p> <p>logical—Use the logical interface description. Only available for MX Series platform configuration.</p>

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443• Example: Setting Up DHCP Option 82 on page 433• RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046

use-interface-description

Syntax	<code>use-interface-description (logical device);</code>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> (relay-agent-interface-id relay-agent-remote-id)], [edit forwarding-options dhcp-relay relay-option-82 (circuit-id remote-id)], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 (circuit-id remote-id)], [edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)], [edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)], [edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-18], [edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-37]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Support at the <code>[edit ... dhcpv6]</code> hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p> <p>Support at the <code>[edit ... relay-agent-remote-id]</code> and <code>[edit ... remote-id]</code> hierarchy levels introduced in Junos OS Release 14.1.</p> <p>Support at the <code>[edit vlans <i>vlan-name</i> dhcp-security dhcpv6-options option-18]</code> and <code>[edit vlans <i>vlan-name</i> dhcp-security dhcpv6-options option-37]</code> hierarchy levels introduced in Junos OS Release 14.1X53-D10 for EX Series switches.</p>
Description	<p>Use the textual interface description instead of the interface identifier in the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or in the DHCPv6 option 18 (Relay Agent Interface ID) or option 37 (Relay Agent Remote ID) information in DHCP packets that the DHCP relay agent sends to a DHCP server.</p>



NOTE: For integrated routing and bridging (IRB) interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID. You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

The textual description is configured using the **description** statement at the `[edit interfaces interface-name]` hierarchy level. If you specify that the textual description be used and no description is configured for the interface, DHCP relay defaults to using the Layer 2

interface name. When you use the interface description rather than the interface name, the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used. To include the IRB interface description instead of the Layer 2 interface description, configure the **use-interface-description** and the **no-vlan-interface-name** statements. If no description is configured for the IRB interface, DHCP relay defaults to using the IRB interface name.



NOTE: The **use-interface-description** statement is mutually exclusive with the **use-vlan-id** statement.

If you specify the textual interface description, rather than accepting the default syntax, the identification is for packets returned from the server, and only for instances where that identification would be required by the DHCP relay, such as a stateless pass-through.



NOTE: By default, DHCP relay accepts a maximum of 253 ASCII characters. If the textual interface description exceeds 253 characters, DHCP relay drops the packet, which results in the DHCP client failing to bind.

Options **logical**—Use the textual description that is configured for the logical interface.
device—Use the textual description that is configured for the device interface.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- *Including a Textual Description in DHCP Options*
- *Using DHCP Relay Agent Option 82 Information*
- *Configuring DHCPv6 Relay Agent Options*

use-interface-index

Syntax	<code>use-interface-index (logical device);</code>
Hierarchy Level	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-18],</code> <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-37],</code>
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Use the index number of the interface instead of the interface name in the DHCPv6 option 18 (Relay Agent Interface-ID) or option 37 (Relay Agent Remote-ID). These options are used by a relay agent to insert information in DHCPv6 requests before the relay agent forwards them to a DHCPv6 server.
Options	logical —Use the textual description that is configured for the logical interface. device —Use the textual description that is configured for the device interface.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Including a Textual Description in DHCP Options</i> • <i>Using DHCP Relay Agent Option 82 Information</i> • <i>Configuring DHCPv6 Relay Agent Options</i>

use-interface-name

Syntax	use-interface-name (logical device);
Hierarchy Level	[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-18], [edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-37],
Release Information	Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Configure DHCPv6 option 18 (Relay Agent Interface-ID) or option 37 (Relay Agent Remote-ID) to use the interface name to identify the port identity of the DHCP client to the DHCP server.
Options	logical —Use the name that is configured for the logical interface. device —Use the name that is configured for the device interface.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Including a Textual Description in DHCP Options</i>• <i>Using DHCP Relay Agent Option 82 Information</i>• <i>Configuring DHCPv6 Relay Agent Options</i>

use-string

Syntax	<code>use-string <i>string</i>;</code>
For Platforms with Enhanced Layer 2 Software (ELS)	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 remote-id]</code>
For Platforms Without ELS	<code>[edit ethernet-switching-options secure-access-port <i>vlan</i> (all <i>vlan-name</i>) dhcp-option82 remote-id],</code> <code>[edit forwarding-options helpers bootp dhcp-option82 remote-id],</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82 remote-id]</code>
For MX Series Platforms	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82 circuit-id]</code>
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Hierarchy level <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.) Hierarchy level <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.
Description	Use a string rather than the MAC address of the host system (the default) in the remote ID value in the DHCP option 82 information.
Options	<i>string</i> —Character string used as the remote ID value. Range: 1–255 characters
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring DHCP Option 82 on a Router with Bridge Domain on page 437 • Example: Setting Up DHCP Option 82 on page 433 • RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046

use-vlan-id

Syntax	<code>use-vlan-id;</code>
For Platforms with Enhanced Layer 2 Software (ELS)	<code>[edit forwarding-options helpers bootp dhcp-option82-circuit-id]</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82-circuit-id]</code>
For MX Series Platforms	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82 circuit-id]</code>
Release Information	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Hierarchy level <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Hierarchy level <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.</p>



NOTE: The EX Series switches that support the `use-vlan-id` statement are the EX4300, EX4600, and EX9200 switches.

Description Use the VLAN ID rather than the VLAN name (the default) in the circuit ID or remote ID value in the DHCP option 82 information.



NOTE: The `use-vlan-id` statement is mutually exclusive with the `use-interface-description` and `no-vlan-interface-name` statements.

The `use-vlan-id` statement only applies to interfaces in a bridge domain. The format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces is as follows:

```
(fe | ge)-fpc/pic/port.subunit:svlan_id-vlan_id
```



NOTE: The *subunit* is required and used to differentiate the interface for remote systems, and *svlan_id-vlan_id* represents the VLANs associated with the bridge domain.

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443 • Example: Setting Up DHCP Option 82 on page 433 • RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046.

validity-period

Syntax	validity-period <i>days</i> ;
Hierarchy Level	[edit security pki auto-re-enrollment certificate-id]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Certificate validity period, in days, from the enrollment start date. If not specified, the issuing certificate authority (CA) sets this time as per its own policy. The start time is when auto-reenrollment is initiated.
Options	<p>days—Number of days that the certificate is valid.</p> <p>Range: 1 through 4095 days</p> <p>Default: Per CA policy</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Auto-Reenrollment of a Router Certificate on page 191 • auto-re-enrollment on page 679

vendor-id

Syntax	<code>vendor-id <string>;</code>
For Platforms with Enhanced Layer 2 Software (ELS)	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82]</code>
For Platforms Without ELS	<code>[edit ethernet-switching-options secure-access-port <i>vlan</i> (all <i>vlan-name</i>) dhcp-option82],</code> <code>[edit forwarding-options helpers bootp dhcp-option82],</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82]</code>
For MX Series Platforms	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82]</code>
Release Information	<p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Hierarchy level <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 13.2X50-D10. (See <i>Using the Enhanced Layer 2 Software CLI</i> for information about ELS.)</p> <p>Hierarchy level <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> introduced in Junos OS Release 14.1 for the MX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Insert a vendor ID in the DHCP option 82 information in a DHCP request packet header before forwarding or relaying the request to a DHCP server.
Default	If vendor-id is not explicitly configured for DHCP option 82, then no vendor ID is set.
Options	<p>string—(Optional) A single string that designates the vendor ID.</p> <p>Range: 1–255 characters</p> <p>Default: If you specify vendor-id with no string value, then the default vendor ID Juniper Networks is configured.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring DHCP Option 82 on a Router with Bridge Domain on page 437 • Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443 • Example: Setting Up DHCP Option 82 on a VLAN on page 433 • Setting Up DHCP Option 82 on the Switch with No Relay (ELS) on page 439

violation-report-rate (DDoS Flow Detection)

Syntax	<code>violation-report-rate <i>report-rate</i>;</code>
Hierarchy Level	<code>[edit system ddos-protection global]</code>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Limit the rate at which bandwidth violations (violation reports) are reported from an FPC to the Routing Engine, for all protocol groups and packet types on all line cards.
Options	<p><i>report-rate</i>—Number of violations per second.</p> <p>Range: 1 through 50,000</p> <p>Default: 100</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types on page 574 • <i>Configuring Flow Detection for DDoS Protection</i>

vlan (Access Port Security)

Syntax

```
vlan (all | vlan-name) {
  (arp-inspection | no-arp-inspection) {
    forwarding-class class-name;
  }
  dhcp-option82 {
    circuit-id {
      prefix hostname;
      use-interface-description;
      use-vlan-id;
    }
    remote-id {
      prefix hostname | mac | none;
      use-interface-description;
      use-string string;
    }
    vendor-id <string>;
  }
  (examine-dhcp | no-examine-dhcp) {
    forwarding-class class-name;
  }
  (examine-dhcpv6 | no-examine-dhcpv6) {
    forwarding-class class-name;
  }
  examine-fip {
    fc-map fc-map-value;
  }
  (ip-source-guard | no-ip-source-guard);
  (ipv6-source-guard | no-ipv6-source-guard);
  mac-move-limit limit action (drop | log | none | shutdown);
}
(neighbor-discovery-inspection | no-neighbor-discovery-inspection);
no-option37;
}
```

Hierarchy Level [edit [ethernet-switching-options secure-access-port](#)]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for the **examine-dhcpv6**, **no-option37**, **neighbor-discovery-inspection**, and **ipv6-source-guard** statements introduced in Junos OS Release 14.1x53-D10 for EX Series switches.

Description Apply any of the following security options to a VLAN:

- DHCP snooping
- DHCPv6 snooping with DHCP option 37
- DHCP option 82
- Dynamic ARP inspection (DAI)

- IPv6 neighbor discovery inspection
- FIP snooping
- IP source guard
- IPv6 source guard
- MAC move limiting

The remaining statements are explained separately. See [CLI Explorer](#).



TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type ? after vlan or vlans in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

Options **all**—Apply the feature to all VLANs.

vlan-name—Apply the feature to the specified VLAN.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 476](#)
- [Example: Setting Up DHCP Option 82 Using the Same VLAN on page 443](#)
- [Example: Configuring an FCoE Transit Switch](#)

vlan (DHCP Bindings on Access Ports)

Syntax	<code>vlan <i>vlan-name</i>;</code>
Hierarchy Level	[edit <code>ethernet-switching-options secure-access-port interface</code> (all <i>interface-name</i>) <code>static-ip ip-address</code>]
Release Information	Statement introduced in Junos OS Release 9.2 for EX Series switches.
Description	Associate the static IP address with the specified VLAN associated with the specified interface.
Options	<i>vlan-name</i> —Name of a specific VLAN associated with the specified interface.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static DHCP IP Addresses for DHCP snooping (non-ELS) on page 405

vlan (RA Guard)

Syntax	<pre>vlan (vlan-name all) { policy policy-name (stateful stateless); }</pre>
Hierarchy Level	[edit forwarding-options access-security router-advertisement-guard]
Release Information	Statement introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Statement introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Configure IPv6 Router Advertisement (RA) guard on a VLAN. In an IPv6 deployment, RA guard protects against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. An RA guard policy is used to validate incoming RA messages on the basis of whether they match the conditions defined in a policy.</p> <p>Before you can configure RA guard on a VLAN, you must first configure a policy at the [edit forwarding-options access-security router-advertisement-guard] hierarchy level. The policy is then applied to the VLAN at the [edit forwarding-options access-security router-advertisement-guard vlans vlan-name] hierarchy level.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateless IPv6 Router Advertisement Guard on page 517 • Configuring Stateful IPv6 Router Advertisement Guard on page 514

vlan (Secure Access Port)

```
Syntax  vlan (all | vlan-name) {
    examine-fip {
        examine-vn2vn {
            beacon-period milliseconds;
        }
        fc-map fc-map-value;
        no-fip-snooping-scaling;
    }
    dhcp-option82
    circuit-id {
        prefix (Circuit ID for Option 82) hostname;
        use-interface-description;
        use-vlan-id;
    }
    remote-id {
        prefix (Remote ID for Option 82) hostname | mac | none;
        use-interface-description;
        use-string string;
    }
    vendor-id <string>;
}
(arp-inspection | no-arp-inspection);
circuit-id {
    prefix (Circuit ID for Option 82) hostname;
    use-interface-description;
    use-vlan-id;
}
remote-id {
    prefix (Remote ID for Option 82) hostname | mac | none;
    use-interface-description;
    use-string string;
}
vendor-id <string>;
}
(examine-dhcp | no-examine-dhcp);
mac-move-limit limit action action;
}
```

Hierarchy Level [edit [ethernet-switching-options](#) secure-access-port]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Apply DHCP snooping, dynamic ARP inspection (DAI), DHCP option 82, and MAC move limiting.



TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type ? after vlan or vlans in your

configuration mode command line. Note that only one VLAN is displayed for a VLAN range.


.....
The remaining statements are explained separately. See [CLI Explorer](#).

Options	<p>all—Apply DHCP snooping, DAI, DHCP option 82, and MAC move limiting to all VLANs.</p> <p>vlan-name —Apply DHCP snooping, DAI, DHCP option 82, and MAC move limiting to the specified VLAN.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding How to Protect Access Ports from Common Attacks on page 6 • Understanding MAC Limiting and MAC Move Limiting for Port Security • Understanding and Using Trusted DHCP Servers on page 371 • Configuring MAC Limiting (QFX Switches) on page 344 • Understanding and Using Trusted DHCP Servers on page 371

vlan (Static IP)

Syntax	<code>vlan <i>vlan-name</i>;</code>
Hierarchy Level	<code>[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>) static-ip <i>ip-address</i>]</code>
Release Information	Statement introduced in Junos OS Release 12.1 for the QFX Series switches.
Description	Associate a static IP address with the specified VLAN.
Options	vlan-name —Name of a VLAN associated with the specified interface.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static DHCP IP Addresses for DHCP snooping (non-ELS) on page 405

vlan (Unknown Unicast Forwarding)

Syntax	<code>vlan (all <i>vlan-name</i>) { interface (Unknown Unicast Forwarding) interface-name; }</code>
Hierarchy Level	[edit ethernet-switching-options unknown-unicast-forwarding]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches. Statement updated with enhanced ? (CLI completion feature) functionality in Junos OS Release 9.5 for EX Series switches.
Description	Specify a VLAN from which unknown unicast packets will be forwarded or specify that the packets will be forwarded from all VLANs. Unknown unicast packets are forwarded from a VLAN to a specific trunk interface. The interface statement is explained separately.
	<div>  <p>TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type ? after <code>vlan</code> or <code>vlangs</code> in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.</p> </div>
Options	<p><code>all</code>—All VLANs.</p> <p><code><i>vlan-name</i></code>—Name of a VLAN.</p>
Required Privilege Level	<p><code>system</code>—To view this statement in the configuration.</p> <p><code>system-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> show vlans show ethernet-switching table on page 1198 Configuring Unknown Unicast Forwarding (CLI Procedure) on page 618 Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 617 <i>OBSOLETE: Understanding Unknown Unicast Forwarding</i>

voip-mac-exclusive

Syntax	voip-mac-exclusive;
Hierarchy Level	[edit ethernet-switching-options secure-access-port interface (all <i>interface-name</i>)]
Release Information	Statement introduced in JUNOS Release 13.2X50-D10.
Description	<p>Restrict a VoIP client MAC address to be learned only in a configured VoIP VLAN.</p> <p>If the voip-exclusive-mac statement is configured at the [edit ethernet-switching-options secure-access-port interface <i>interface-name</i>] hierarchy level for an interface in a VoIP VLAN, any MAC address learned on that interface for the VoIP VLAN is not learned on an interface for a data VLAN. If a MAC address has been learned on a data VLAN interface and then later, is learned on a VoIP VLAN with that same interface, the MAC address is removed from the data VLAN interface.</p>
Default	A client MAC address is unrestricted and can be learned on both a VoIP VLAN and a data VLAN.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Port Security (non-ELS) on page 11 • secure-access-port on page 979

write-interval

Syntax	<code>write-interval <i>seconds</i>;</code>
For Platforms with Enhanced Layer 2 Software (ELS)	[edit system processes dhcp-service dhcp-snooping-file], [edit system processes dhcp-service dhcpv6-snooping-file]
For Platforms Without ELS	[edit ethernet-switching-options secure-access-port dhcp-snooping-file], [edit ethernet-switching-options secure-access-port dhcpv6-snooping-file]
For MX Series Platforms	[edit system processes dhcp-service dhcp-snooping-file]
Release Information	<p>Statement introduced in Junos OS Release 9.4 for EX Series switches.</p> <p>Support at the [edit system processes dhcp-service dhcp-snooping-file] hierarchy level introduced in Junos OS Release 13.2X50-D10.</p> <p>Support at the [edit system processes dhcp-service dhcpv6-snooping-file] hierarchy level introduced in Junos OS Release 13.2X51-D20.</p> <p>Statement introduced in Junos OS Release 14.1 for the MX Series.</p> <p>Support at the [edit ethernet-switching-options secure-access-port dhcpv6-snooping-file] hierarchy level introduced in Junos OS Release 14.1X53-D10 for EX Series switches.</p>
Description	<p>Specify how frequently the device writes the database entries from memory into the DHCP snooping database file.</p> <ul style="list-style-type: none"> If you are configuring write-interval at the [edit system processes dhcp-service dhcp-snooping-file] or the [edit system processes dhcp-service dhcpv6-snooping-file] hierarchy level, see “Configuring Persistent Bindings in the DHCP or DHCPv6 (ELS)” on page 381.
Options	<p>seconds—Value in seconds.</p> <p>Range: 60 through 86,400 seconds.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Understanding DHCP Snooping (non-ELS) on page 393

CHAPTER 28

Operational Commands

- clear security host-vpn security-associations
- clear security pki certificate-request
- clear access-security router-advertisement statistics
- clear arp
- clear arp inspection statistics
- clear bridge recovery-timeout
- clear ddos-protection protocols
- clear dhcp snooping binding
- clear dhcp snooping statistics
- clear dhcp-security binding
- clear dhcp-security ipv6 binding
- clear dhcpv6 snooping binding
- clear dhcpv6 snooping statistics
- clear dot1x
- clear ethernet-switching port-error
- clear ethernet-switching recovery-timeout
- clear ethernet-switching table
- clear neighbor-discovery-inspection statistics
- show security macsec connections
- clear security mka statistics
- clear security mka statistics (MX Series)
- clear security pki ca-certificate
- clear security pki crl
- clear security pki key-pair
- clear security pki local-certificate
- clear services ipsec-vpn certificates
- clear services ipsec-vpn ike security-associations
- clear services ipsec-vpn ipsec security-associations

- clear services ipsec-vpn ipsec statistics
- request access-security router-advertisement-guard-block
- request access-security router-advertisement-guard-forward
- request access-security router-advertisement-guard-learn interface
- request ipsec switch
- request security certificate enroll (Signed)
- request security certificate enroll (Unsigned)
- request security key-pair
- request security pki ca-certificate enroll
- request security pki ca-certificate load
- request security pki ca-certificate verify
- request security pki crl load
- request security pki generate-certificate-request
- request security pki generate-key-pair
- request security pki local-certificate enroll
- request security pki local-certificate generate-self-signed
- request security pki local-certificate load
- request security pki local-certificate verify
- request system certificate add
- show access-security router-advertisement state
- show access-security router-advertisement statistics
- show arp inspection statistics
- show ddos-protection protocols
- show ddos-protection protocols parameters
- show ddos-protection protocols statistics
- show ddos-protection protocols violations
- show ddos-protection statistics
- show ddos-protection version
- show dhcp snooping binding
- show dhcp snooping statistics
- show dhcp-security arp inspection statistics
- show dhcp-security binding
- show dhcp-security binding ip-source-guard
- show dhcp-security ipv6 binding
- show dhcp-security ipv6 statistics
- show dhcp-security neighbor-discovery-inspection statistics
- show dhcpv6 snooping binding

- `show dhcpv6 snooping statistics`
- `show ethernet-switching table`
- `show ike security-associations`
- `show ipsec certificates`
- `show ipsec security-associations`
- `show ip-source-guard`
- `show ipv6-source-guard`
- `show neighbor-discovery-inspection statistics`
- `show security host-vpn security-associations`
- `show security host-vpn version`
- `show security keychain`
- `show security macsec connections (MX Series)`
- `show security macsec statistics`
- `include-sci (MACsec for MX Series) on page 1250`
- `show security mka sessions`
- `show security mka sessions (MX Series)`
- `show security mka sessions summary`
- `show security mka statistics`
- `show security pki ca-certificate`
- `show security pki certificate-request`
- `show security pki crt`
- `show security pki local-certificate`
- `show services ipsec-vpn certificates`
- `show services ipsec-vpn ike security-associations`
- `show services ipsec-vpn ipsec security-associations`
- `show services ipsec-vpn ipsec statistics`
- `show system certificate`
- `show system statistics arp`

clear security host-vpn security-associations

Syntax	<code>clear security host-vpn security-associations <i>connection-name</i></code>
Release Information	Statement introduced in Junos OS Evolved Release 18.3R1.
Description	Clear IPsec security association information for the security association specified.
Options	<i>connection-name</i> —Specify the protection information to be cleared by connection name. If no connection name is specified, information for all security associations is cleared.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show security host-vpn security-associations on page 1236• host-vpn on page 800
List of Sample Output	clear security host-vpn security-associations connection-name on page 1070 clear security host-vpn security-associations on page 1070

Sample Output

clear security host-vpn security-associations connection-name

```
user@host> clear security host-vpn security-associations leftT1
terminate of sa:leftT1 complete
```

clear security host-vpn security-associations

```
user@host> clear security host-vpn security-associations
terminate without IKE-SA name unsupported
```

clear security pki certificate-request

Syntax	clear security pki certificate-request (all certificate-id <i>certificate-id-name</i>)
Release Information	Command introduced in Junos OS Release 7.5.
Description	Delete manually generated local digital certificate requests from the router.
Options	<p>all—Delete all local digital certificate requests from the router.</p> <p>certificate-id <i>certificate-id-name</i>—Delete the specified local digital certificate and corresponding public/private key pair.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show security pki certificate-request on page 1264
List of Sample Output	clear security pki certificate-request all on page 1071
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki certificate-request all

```
user@host> clear security pki certificate-request all
```

clear access-security router-advertisement statistics

Syntax	<code>clear access-security router-advertisement statistics (fail success) (all interface <i>interface-name</i> vlan <i>vlan-name</i>)</code>
Release Information	Command introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Command introduced in Junos OS Release 16.1 for EX Series switches.
Description	Clear the IPv6 Router Advertisement (RA) guard entries for received RA messages. If RA guard is enabled on a switch, the switch examines incoming RA messages and filters them on the basis of a predefined set of criteria. If the switch validates the sender of the RA message as a legitimate IPv6 router, it forwards the RA message to its destination; otherwise, the RA message is dropped.
Options	all —Clear the RA guard entries on all VLANs. fail —Clear RA guard entries for RA messages that were discarded. interface <i>interface-name</i> —Clear the RA guard entries for the specified interface. success —Clear the RA guard entries for RA messages that were accepted. vlan <i>vlan-name</i> —Clear the RA guard entries for the specified VLAN.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show access-security router-advertisement statistics on page 1128
Output Fields	This command generates no output.

clear arp

Syntax	<pre>clear arp <all> <hostname <i>hostname</i>> <interface <i>interface-name</i>> <logical-system <i>logical-system-name</i>> <tenant <i>name</i>> <vpn <i>vpn</i>></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 14.1 for the MX Series.</p> <p>all option introduced in Junos OS Release 14.2.</p> <p>tenant option added in Junos OS Release 18.3.</p>
Description	<p>Remove entries from the Address Resolution Protocol (ARP) table for the current CLI view. To clear entries for a specific logical system, you must first enter the set cli logical-system <i>logical-system-name</i> command, and then issue the clear arp command.</p>
Options	<p>all— Clear all entries from the ARP table.</p> <p>hostname <i>hostname</i>—(Optional) Clear only the specified host entry from the ARP table.</p> <p>interface <i>interface-name</i>—(Optional) Clear entries only for the specified interface from the ARP table.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Clear entries for only the specified logical system from the ARP table (only available in main router context).</p> <p>tenant <i>name</i>—(Optional) Clear entries for only the specified tenant from the ARP table (only available in main router context).</p> <p>vpn <i>vpn</i>—(Optional) Clear entries from the ARP table for the specified virtual private network (VPN).</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • set cli logical-system • show arp • show dhcp-security arp inspection statistics on page 1181 • Port Security Features on page 3
List of Sample Output	<p>clear arp all on page 1074</p> <p>clear arp logical-system ls1 on page 1074</p>

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear arp all

```
user@host> clear arp all
192.168.71.254    deleted
192.168.65.46    deleted
192.168.64.10    deleted
10.0.12.14       deleted
10.0.17.14       deleted
```

clear arp logical-system ls1

```
user@host> clear arp logical-system ls1
192.168.71.254    deleted
192.168.65.46    deleted
192.168.64.10    deleted
10.0.12.14       deleted
10.0.17.14       deleted
```

clear arp inspection statistics

Syntax	clear arp inspection statistics <interface <i>interface</i> >
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 12.1 for the QFX Series.
Description	Clear ARP inspection statistics.
Options	none —Clears ARP statistics on all interfaces. interface <i>interface-names</i> —(Optional) Clear ARP statistics on one or more interfaces.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show arp inspection statistics on page 1130 • Example: Configuring Port Security (non-ELS) on page 15 • Verifying That DAI Is Working Correctly on page 453
List of Sample Output	clear arp inspection statistics on page 1075
Output Fields	This command produces no output.

Sample Output

clear arp inspection statistics

```
user@switch> clear arp inspection statistics
```

clear bridge recovery-timeout

Syntax `clear bridge recovery-timeout
<interface interface-name>`

Release Information Command introduced in Junos OS Release 14.1 for MX Series routers.

Description Clear all storm control errors from all the Ethernet switching interfaces on the switch, and restore the interfaces to service.

Options **interface *interface-name***—Clear all storm control errors from the Ethernet switching interfaces on the interface specified in the command and restore this interface to service.

Required Privilege Level clear

Related Documentation

- [Configuring Autorecovery for Port Security Events on page 635](#)

List of Sample Output [clear bridge recovery-timeout \(interface interface-name\) on page 1076](#)

Sample Output

`clear bridge recovery-timeout (interface interface-name)`

```
user@host> clear bridge recovery-timeout interface ae0.0
user@host> clear bridge recovery-timeout interface ae0.0
```


clear ddos-protection protocols

Syntax	clear ddos-protection protocols <protocol-group <packet-type>> (culprit-flows states statistics)
Release Information	<p>Command introduced in Junos OS Release 11.2.</p> <p>Option culprit-flows introduced in Junos OS Release 12.3.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 14.1X53 on QFX Series switches.</p> <p>Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.</p>
Description	Clear current DDoS protection statistics, violation states, or culprit flows for all packet types in all protocol groups, for all packet types in a particular protocol group, or for a particular packet type in a particular protocol group.
Options	<p>protocol-group—(Optional) Protocol group that is cleared. See show ddos-protection protocols for a list of available groups.</p> <p>packet-type—(Optional) Packet type in a particular protocol group that is cleared. See show ddos-protection protocols for a list of available packet types.</p> <p>culprit-flows—Clear culprit flows for a packet type, for a protocol group, or for all protocol groups. This option is not supported on QFX Series switches.</p> <p>states—Clear DDoS protection violation states for a packet type, for a protocol group, or for all protocol groups.</p> <p>statistics—Clear DDoS protection statistics such as packet counts and rates for a packet type, for a protocol group, or for all protocol groups.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show ddos-protection protocols on page 1132 • show ddos-protection statistics on page 1174 • show ddos-protection version on page 1176
List of Sample Output	clear ddos-protection protocols (Clear Statistics for All Protocols) on page 1078 clear ddos-protection protocols (Clear Violation States for Packet Type) on page 1078
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ddos-protection protocols (Clear Statistics for All Protocols)

```
user@host> clear ddos-protection protocols statistics
```

clear ddos-protection protocols (Clear Violation States for Packet Type)

```
user@host> clear ddos-protection protocols radius server states
```

clear dhcp snooping binding

Syntax	<pre>clear dhcp snooping binding <mac (all <i>mac-address</i>)> <vlan (all <i>vlan-name</i>)> <vlan (all <i>vlan-name</i>) mac (all <i>mac-address</i>)></pre>
Release Information	<p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 12.1 for the QFX Series.</p>
Description	Clear the DHCP snooping database information.
Options	<p>mac (all <i>mac-address</i>)—(Optional) Clear DHCP snooping information for the specified MAC address or all MAC addresses.</p> <p>vlan (all <i>vlan-name</i>)—(Optional) Clear DHCP snooping information for the specified VLAN or all VLANs.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show dhcp snooping binding on page 1178 • Example: Configuring Port Security (non-ELS) on page 15 • Enabling DHCP Snooping (non-ELS) on page 400
List of Sample Output	clear dhcp snooping binding on page 1079
Output Fields	This command produces no output.

Sample Output

clear dhcp snooping binding

```
user@switch> clear dhcp snooping binding
```

clear dhcp snooping statistics

Syntax	<code>clear dhcp snooping statistics</code>
Release Information	Command introduced in Junos OS Release 9.4 for EX Series switches.
Description	Clear all Dynamic Host Configuration Protocol (DHCP) snooping statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show dhcp snooping statistics on page 1180• Understanding DHCP Snooping (non-ELS) on page 393
List of Sample Output	clear dhcp snooping statistics on page 1080
Output Fields	See show dhcp snooping statistics for an explanation of the output fields.

Sample Output

clear dhcp snooping statistics

The following sample output displays the DHCP snooping statistics before and after the `clear dhcp snooping statistics` command is issued.

```
user@switch> show dhcp snooping statistics
```

Successful Transfers :	0	Failed Transfers :	21
Successful Reads :	0	Failed Reads :	0
Successful Writes :	0	Failed Writes :	21

```
user@switch> clear dhcp snooping statistics
```

```
user@switch> show dhcp snooping statistics
```

Successful Transfers :	0	Failed Transfers :	0
Successful Reads :	0	Failed Reads :	0
Successful Writes :	0	Failed Writes :	0

clear dhcp-security binding

Syntax	<pre>clear dhcp-security binding <interface <i>interface-name</i>> <ip-address <i>ip-address</i>> <statistics> <vlan <i>vlan-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Command introduced in Junos OS Release 14.1 for the MX Series.</p>
Description	Clear the DHCP snooping database information.
Options	<p>interface <i>interface-name</i>—(Optional) Clear DHCP snooping database information for the specified interface.</p> <p>ip-address <i>ip-address</i>—(Optional) Clear DHCP snooping database information for the specified IP address.</p> <p>statistics—(Optional) Clear all DHCP snooping database statistics.</p> <p>vlan <i>vlan-name</i>—(Optional) Clear DHCP snooping database information for the specified VLAN.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show dhcp-security binding on page 1183 • Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487 • Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 497 • Port Security Features on page 3

clear dhcp-security ipv6 binding

Syntax	<pre>clear dhcp-security ipv6 binding <all> <interface <i>interface-name</i>> <ipv6-address <i>ipv6-address</i>> <vlan <i>vlan-name</i>></pre>
Release Information	Command introduced in Junos OS Release 13.2X51-D20 for EX Series switches.
Description	Clear the DHCPv6 snooping database information.
Options	<p>all—(Optional) Clear all DHCPv6 snooping database statistics.</p> <p>interface <i>interface-name</i>—(Optional) Clear DHCPv6 snooping database information for the specified interface.</p> <p>ipv6-address <i>ipv6-address</i>—(Optional) Clear DHCPv6 snooping database information for the specified IPv6 address.</p> <p>vlan <i>vlan-name</i>—(Optional) Clear DHCPv6 snooping database information for the specified VLAN.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show dhcp-security ipv6 binding on page 1188• Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 492
List of Sample Output	clear dhcp-security ipv6 binding on page 1082
Output Fields	This command produces no output.

Sample Output

clear dhcp-security ipv6 binding

```
user@switch> clear dhcp-security ipv6 binding
```

clear dhcpv6 snooping binding

Syntax	<pre>clear dhcpv6 snooping binding <mac (all <i>mac-address</i>)> <vlan (all <i>vlan-name</i>)> <vlan (all <i>vlan-name</i>) mac (all <i>mac-address</i>)></pre>
Release Information	Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Clear the DHCPv6 snooping database information.
Options	<p>mac (all <i>mac-address</i>)—(Optional) Clear DHCPv6 snooping information for the specified MAC address or all MAC addresses.</p> <p>vlan (all <i>vlan-name</i>)—(Optional) Clear DHCPv6 snooping information for the specified VLAN or all VLANs.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show dhcpv6 snooping binding on page 1195 • Example: Configuring Port Security (non-ELS) on page 15 • Enabling DHCP Snooping (non-ELS) on page 400
List of Sample Output	clear dhcpv6 snooping binding on page 1083
Output Fields	This command produces no output.

Sample Output

clear dhcpv6 snooping binding

```
user@switch> clear dhcpv6 snooping binding
```

clear dhcpv6 snooping statistics

Syntax	<code>clear dhcpv6 snooping statistics</code>
Release Information	Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Clear all Dynamic Host Configuration Protocol for IPv6 (DHCPv6) snooping statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show dhcpv6 snooping statistics on page 1197• Understanding DHCP Snooping (non-ELS) on page 393
List of Sample Output	clear dhcpv6 snooping statistics on page 1084
Output Fields	See show dhcpv6 snooping statistics for an explanation of the output fields.

Sample Output

clear dhcpv6 snooping statistics

The following sample output displays the DHCPv6 snooping statistics before and after the `clear dhcpv6 snooping statistics` command is issued.

```
user@switch> show dhcpv6 snooping statistics
```

Successful Transfers :	0	Failed Transfers :	21
Successful Reads :	0	Failed Reads :	0
Successful Writes :	0	Failed Writes :	21

```
user@switch> clear dhcpv6 snooping statistics
```

```
user@switch> show dhcpv6 snooping statistics
```

Successful Transfers :	0	Failed Transfers :	0
Successful Reads :	0	Failed Reads :	0
Successful Writes :	0	Failed Writes :	0

clear dot1x

Syntax `clear dot1x (firewall <counter-name> | interface <[interface-name]> | mac-address [mac-addresses] | statistics <interface interface-name>)`

Release Information Command introduced in Junos OS Release 9.0 for EX Series switches.
firewall option added in Junos OS Release 9.5 for EX Series switches.
 Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.
 Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
 Support for **eapol-block** introduced in Junos OS Releases 14.1X53-D40 and 15.1X53-D51 for EX Series switches.

Description Reset the authentication state of an interface or delete 802.1X statistics from the switch. When you reset an interface using the **interface** or **mac-address** options, reauthentication on the interface is also triggered. The switch sends out a multicast message on the interface to restart the authentication of all connected supplicants. If a MAC address is reset, then the switch sends out a unicast message to that specific MAC address to restart authentication.

If a supplicant is sending traffic when the **clear dot1x interface** command is issued, the authenticator immediately initiates reauthentication. This process happens quickly, and it might seem that reauthentication did not occur. To verify that reauthentication has happened, issue the **show dot1x interface detail** command. The values for **Reauthentication due** and **Reauthentication interval** will be about the same.



CAUTION: When you clear the learned MAC addresses from an interface using the **clear dot1x interface** command, all MAC addresses are cleared, including those in static MAC bypass list.

If you have enabled Media Access Control Security (MACsec) using static secure association key (SAK) security mode on an EX Series switch, the SAKs are rotated when the **clear dot1x** command is entered. The **clear dot1x** command has no impact on MACsec when MACsec is enabled using static connectivity association keys (CAK) or any other security mode.

Options **eapol-block**—Clear EAPOL block on the interface and allow the switch to receive EAPOL messages from a supplicant connected to that interface.

firewall <counter-name>—Clear 802.1X firewall counter statistics. If the *counter-name* option is specified, clear 802.1X firewall statistics for that counter.

interface <[interface-name]>—Reset the authentication state of all the supplicants (also, clears all the authentication bypassed clients) connected to the specified

interface (when the interface is an authenticator) or reset the authentication state for the interface itself (when the interface is a supplicant).

mac-address [*mac-addresses*]*—Reset the authentication state of the specified MAC addresses.*

statistics <interface *interface-name*>*—Clear 802.1X statistics on all 802.1X-enabled interfaces. If the interface option is specified, clear 802.1X firewall statistics for that interface or interfaces.*

Required Privilege Level

view

Related Documentation

- *show dot1x*
- *Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch*
- *Filtering 802.1X Supplicants by Using RADIUS Server Attributes*

List of Sample Output

[clear dot1x firewall on page 1086](#)
[clear dot1x interface \(Specific Interfaces\) on page 1086](#)
[clear dot1x mac-address \(Specific MAC Address\) on page 1086](#)
[clear dot1x statistics interface \(Specific Interface\) on page 1086](#)
[clear dot1x eapol-block on page 1086](#)

Sample Output

clear dot1x firewall

```
user@switch> clear dot1x firewall c1
```

clear dot1x interface (Specific Interfaces)

```
user@switch> clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0
```

clear dot1x mac-address (Specific MAC Address)

```
user@switch> clear dot1x mac-address 00:04:ae:cd:23:5f
```

clear dot1x statistics interface (Specific Interface)

```
user@switch> clear dot1x statistics interface ge-1/0/1
```

clear dot1x eapol-block

```
user@switch> clear dot1x eapol-block
```

clear ethernet-switching port-error

Syntax	clear ethernet-switching port-error <interface <i>interface-name</i> >
Release Information	Command introduced in JUNOS Release 9.6 for EX Series switches.
Description	Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch or from the specified interface, and restore all interfaces or the specified interface to service.
Options	<p>none—Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch and restore these interfaces to service.</p> <p>interface <i>interface-name</i>—(Optional) Clear all MAC limiting, MAC move limiting, and storm control errors from the specified interface and restore the interface to service.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • Configuring Autorecovery for Port Security Events on page 635 • Configuring Port Security (non-ELS) on page 11 • Configuring Autorecovery for Port Security Events on page 635
List of Sample Output	clear ethernet-switching port-error on page 1087
Output Fields	This command produces no output.

Sample Output

clear ethernet-switching port-error

```
user@switch> clear ethernet-switching port-error
```

clear ethernet-switching recovery-timeout

Syntax	clear ethernet-switching recovery-timeout
Release Information	Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch, and restore the interfaces to service.
Options	interface <i>interface-name</i> vlan <i>vlan-name</i> —(EX9200 switches) Unblock an interface on the basis of its membership in the specified VLAN. This option can be used to restore an interface that is blocked because of a vlan-member-shutdown action.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• Configuring Autorecovery for Port Security Events on page 635
Output Fields	This command produces no output.

clear ethernet-switching table

Syntax clear ethernet-switching table
 <interface *interface-name*>
 <mac *mac-address*>
 <management-vlan>
 <persistent-mac <*interface* | *mac-address*>>
 <vlan *vlan-name*>

Syntax (QFX Series) clear ethernet-switching table
 <interface *interface-name*>
 <mac *mac-address*>
 <persistent-mac <*interface* | *mac-address*>>
 <vlan *vlan-name*>

Release Information Command introduced in Junos OS Release 9.3 for EX Series switches.
 Command introduced in Junos OS Release 11.1 for the QFX Series.

Description



NOTE: On a QFabric system, using this command on an FCoE-enabled VLAN when FCoE sessions are active can cause traffic flooding and FCoE traffic drop. The FCoE sessions are not terminated and the traffic reconverges after a short period of time.

Clear learned entries, which are media access control (MAC) addresses, in the Ethernet switching table (also called the forwarding database table).

Options **none**—Clear learned entries in the Ethernet switching table, except for persistent MAC addresses.

interface *interface-name*—(Optional) Clear all learned MAC addresses for the specified interface from the Ethernet switching table.

mac *mac-address*—(Optional) Clear the specified learned MAC address from the Ethernet switching table.

management-vlan—(Optional) Clear all MAC addresses learned for the management VLAN from the Ethernet switching table. Note that you do not specify a VLAN name because only one management VLAN exists.

persistent-mac <*interface* | *mac-address*>—(Optional) Clear all MAC addresses, including persistent MAC addresses. Use the **interface** option to clear all MAC addresses on an interface, or use the **mac-address** option to clear all entries for a specific MAC address.

Use this command whenever you move a device in your network that has a persistent MAC address on the switch. If you move the device to another port on the switch and do not clear the persistent MAC address from the original port it was learned on, then the new port will not learn the MAC address and the device will not be able to connect. If the original port is down when you move the device, then the new port will learn the MAC address and the device can connect—however, unless you cleared the MAC address on the original port, when the port comes back up, the system reinstalls the persistent MAC address in the forwarding table for that port. If this occurs, the address is removed from the new port and the device loses connectivity.

vlan *vlan-name*—(Optional) Clear all MAC addresses learned for the specified VLAN from the Ethernet switching table.

Required Privilege Level view

Related Documentation

- [show ethernet-switching table on page 1198](#)

List of Sample Output [clear ethernet-switching table on page 1090](#)

Output Fields This command produces no output.

Sample Output

[clear ethernet-switching table](#)

```
user@switch> clear ethernet-switching table
```

clear neighbor-discovery-inspection statistics

Syntax	clear neighbor-discovery-inspection statistics <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Clear IPv6 neighbor discovery inspection statistics.
Options	<p>none—Clear neighbor discovery inspection statistics on all interfaces.</p> <p>interface <i>interface-name</i>—(Optional) Clear neighbor discovery inspection statistics on one or more interfaces.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show neighbor-discovery-inspection statistics on page 1235 • Example: Configuring Port Security (non-ELS) on page 15
List of Sample Output	clear neighbor-discovery-inspection statistics on page 1091
Output Fields	This command produces no output.

Sample Output

clear neighbor-discovery-inspection statistics

```
user@switch> clear neighbor-discovery-inspection statistics
```

show security macsec connections

Syntax	<code>show security macsec connections</code> <code><interface <i>interface-name</i>></code>
Release Information	Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches. Command introduced in Junos OS Release 18.2R1 for ACX6360 Routers.
Description	Display the status of the active MACsec connections on the switch. This command does not display output when MACsec is enabled using static secure association key (SAK) security mode.
Options	none —Display MACsec connection information for all interfaces on the switch. interface <i>interface-name</i> —(Optional) Display MACsec connection information for the specified interface only.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> show security macsec statistics on page 1246
List of Sample Output	show security macsec connections on page 1093
Output Fields	Table 40 on page 1092 lists the output fields for the show security macsec connections command. Output fields are listed in the approximate order in which they appear.

Table 40: show security macsec connections Output Fields

Field Name	Field Description
Fields for Interface	
Interface name	Name of the interface.
CA name	Name of the connectivity association. A connectivity association is named using the connectivity-association statement when you are enabling MACsec.
Cipher suite	Name of the cipher suite used for encryption.

Table 40: show security macsec connections Output Fields (continued)

Field Name	Field Description
Encryption	<p>Encryption setting. Encryption is enabled when this output is on and disabled when this output is off.</p> <p>The encryption setting is set using the no-encryption statement in the connectivity association when using static connectivity association key (CAK) security mode and is set using the encryption statement in the secure channel when using static secure association key (SAK) or dynamic security mode.</p>
Key server offset	<p>Offset setting.</p> <p>The offset is set using the offset statement when configuring the connectivity association when using static connectivity association key (CAK) or dynamic security mode or the secure channel when using static secure association key (SAK) security mode.</p>
Include SCI	<p>SCI tagging. The SCI tag is included on packets in a secure channel when this output is yes, and not included on packets in a secure channel when this output is no.</p> <p>You can enable SCI tagging using the include-sci statement in the connectivity association.</p> <p>NOTE: SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. The include-sci option is, therefore, not available on EX4300 switches. The output for the Include SCI field is yes.</p>
Replay protect	<p>Replay protection setting. Replay protection is enabled when this output is on and disabled when this output is off.</p> <p>You can enable replay protection using the replay-protect statement in the connectivity association.</p>
Replay window	<p>Replay protection window setting. This output is set to 0 when replay protection is disabled, and is the size of the replay window, in number of packets, when replay protection is enabled.</p> <p>The size of the replay window is configured using the replay-window-size statement in the connectivity association.</p>

Sample Output

show security macsec connections

```
user@host> show security macsec connections
```

```
Interface name: xe-0/1/0
  CA name: CA1
  Cipher suite: GCM-AES-128   Encryption: on
  Key server offset: 0        Include SCI: no
  Replay protect: off         Replay window: 0
```

clear security mka statistics

Syntax	<code>clear security mka statistics</code> <code><interface <i>interface-name</i>></code>
Release Information	Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
Description	<p>Clear—reset to zero (0)—all MACsec Key Agreement (MKA) protocol statistics.</p> <p>You are clearing the statistics that are viewed using the show security mka statistics when you enter this command.</p>
Options	<p>none—Clear all MKA counters for all interfaces on the switch.</p> <p>interface <i>interface-name</i>—(Optional) Clear MKA traffic counters for the specified interface only.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show security mka statistics on page 1258• show security mka sessions on page 1251• Understanding Media Access Control Security (MACsec) on page 217

Sample Output

clear security mka statistics

```
user@switch> clear security mka statistics
```

clear security mka statistics (MX Series)

Syntax clear security mka statistics
 <interface *interface-name*>

Release Information Command introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.

Description Clear—reset to zero (0)—all MACsec Key Agreement (MKA) protocol statistics.

You are clearing the statistics that are viewed using the **show security mka statistics** when you enter this command.

Options **none**—Clear all MKA counters for all interfaces on the switch.

interface *interface-name*—(Optional) Clear MKA traffic counters for the specified interface only.

Required Privilege Level clear

Sample Output

clear security mka statistics

```
user@switch> clear security mka statistics
```

clear security pki ca-certificate

Syntax	clear security pki ca-certificate (all ca-profile <i>ca-profile-name</i>)
Release Information	Command introduced in Junos OS Release 7.5.
Description	Delete certificate authority (CA) digital certificates from the router.
Options	all —Delete all CA digital certificates from the router. ca-profile <i>ca-profile-name</i> —Delete the specified CA profile.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• request security pki ca-certificate enroll on page 1113• request security pki ca-certificate load on page 1114• show security pki ca-certificate on page 1260
List of Sample Output	clear security pki ca-certificate all on page 1096
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki ca-certificate all

```
user@host> clear security pki ca-certificate all
```

clear security pki crt

Syntax	clear security pki crt (all ca-profile <i>ca-profile-name</i>)
Release Information	Command introduced in Junos 8.1
Description	Delete certificate revocation lists (CRLs) from the router.
Options	all —Delete all CRLs from the router. ca-profile <i>ca-profile-name</i> —Delete CRLs associated with the specified CA profile.
Required Privilege Level	clear
List of Sample Output	clear security pki crt ca-profile all on page 1097
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki crt ca-profile all

```
user@host> clear security pki crt ca-profile all
```

clear security pki key-pair

Syntax	clear security pki key-pair (all certificate-id <i>certificate-id-name</i>)
Release Information	Command introduced in Junos OS Release 8.5.
Description	Clear public key infrastructure (PKI) key pair information for local digital certificates from the router.
Options	<p>all—Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.</p> <p>certificate-id <i>certificate-id-name</i>—Delete the specified local digital certificate and corresponding public/private key pair.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• request security pki local-certificate enroll on page 1120• show security pki local-certificate on page 1270
Output Fields	This command produces no output.

Sample Output

```
user@host> clear security pki key pair
```

clear security pki local-certificate

Syntax	clear security pki local-certificate <all certificate-id <i>certificate-id-name</i> system-generated>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the router.
Options	<p>all—(Optional) Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.</p> <p>certificate-id <i>certificate-id-name</i>—(Optional) Delete the specified local digital certificate and corresponding public and private key pair.</p> <p>system-generated—(Optional) Auto-generated self-signed certificate.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • request security pki local-certificate enroll on page 1120 • show security pki local-certificate on page 1270
List of Sample Output	clear security pki local-certificate all on page 1099
Output Fields	This command produces no output.

Sample Output

clear security pki local-certificate all

```
user@host> clear security pki local-certificate all
```

clear services ipsec-vpn certificates

Syntax	clear services ipsec-vpn certificates (all service-set <i>service-set</i>) <certificate-cache-entry <i>number</i> >
Release Information	Command introduced in Junos OS Release 7.5.
Description	(Adaptive services interfaces only) Delete digital certificates from the IPsec configuration memory cache. Issuing this command also clears the certificate revocation list (CRL) from the cache along with the certificates.
Options	all —Delete digital certificates for all service sets. service-set <i>service-set</i> —Delete digital certificates for the specified service set.
Required Privilege Level	clear
List of Sample Output	clear services ipsec-vpn certificates all on page 1100
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn certificates all

```
user@host> clear services ipsec-vpn certificates all
```


clear services ipsec-vpn ike security-associations

Syntax	clear services ipsec-vpn ike security-associations <peer-address-name> <service-set service-set-name>
Release Information	Command introduced before Junos OS Release 7.4. service-set option added in Junos OS Release 8.5.
Description	(Adaptive services interfaces only) Clear Internet Key Exchange (IKE) security associations.
Options	<p>peer-address-name—(Optional) Clear only the security association specified by the peer address.</p> <p>service-set service-set-name—(Optional) Clear only the security association specified by the service-set name.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show services ipsec-vpn ike security-associations on page 1276
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ike security-associations

```
user@host> clear services ipsec-vpn ike security-associations
```

clear services ipsec-vpn ipsec security-associations

Syntax	<pre>clear services ipsec-vpn security-associations <peer-address-name> <remote-gateway remote-gateway-address> <service-set-name> <tunnel-index tunnel-index-number></pre>
Release Information	Command introduced before Junos OS Release 7.4. remote-gateway , service-set-name , and tunnel-index options added in Junos OS Release 8.4.
Description	(Adaptive services interfaces only) Clear IP Security (IPsec) security associations. You can combine the options for greater specificity.
Options	<p>peer-address-name—(Optional) Clear only the security association specified by the peer address.</p> <p>remote-gateway remote-gateway-address—(Optional) Clear only the security association specified by the remote gateway address.</p> <p>service-set-name—(Optional) Clear only the security association specified by the service-set name.</p> <p>tunnel-index tunnel-index-number—(Optional) Clear only the security association specified by the tunnel index number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show services ipsec-vpn ipsec security-associations on page 1281
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ipsec security-associations

```
user@host> clear services ipsec-vpn ipsec security-associations
```

clear services ipsec-vpn ipsec statistics

Syntax	clear services ipsec-vpn ipsec statistics <remote-gateway <i>address</i> > <service-set <i>service-set-name</i> >
Release Information	Command introduced in Junos OS Release 8.1.
Description	(Adaptive services interface only) Clear IP Security (IPsec) statistics.
Options	remote-gateway <i>address</i> —(Optional) Clear statistics for the specified remote system. service-set <i>service-set-name</i> —(Optional) Clear statistics for the specified service set.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show services ipsec-vpn ipsec statistics on page 1287
List of Sample Output	clear services ipsec-vpn ipsec statistics on page 1103
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ipsec statistics

```
user@host> clear services ipsec-vpn ipsec statistics
```

request access-security router-advertisement-guard-block

Syntax	<code>request access-security router-advertisement-guard-block interface <i>interface-name</i></code>
Release Information	Command introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Command introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Initiate the blocking state on an interface or range of interfaces for stateful IPv6 Router Advertisement (RA) guard. Stateful RA guard learns about legitimate senders of RA messages and stores this information in order to validate senders of subsequent RA messages. For example, an interface that is in the learning state and receives RA messages that are not sent from valid IPv6 routers will dynamically transition to the blocking state. While the interface is in blocking state, all RA messages received on that interface are dropped.</p> <p>You can override the dynamic state transitions by requesting the blocking state on an interface. If you issue the request for the blocking state on an interface, the interface will remain in forwarding state until either the learning or forwarding state is requested on that interface.</p>
Options	<code>interface <i>interface-name</i></code> —Initiate the blocking state on the specified interface.
Required Privilege Level	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Stateful IPv6 Router Advertisement Guard on page 514
Output Fields	This command produces no output.

request access-security router-advertisement-guard-forward

Syntax	request access-security router-advertisement-guard-forward interface (<i>interface-name</i>)
Release Information	Command introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Command introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Initiate the forwarding state on an interface or range of interfaces for stateful IPv6 Router Advertisement (RA) guard. Stateful RA guard learns about legitimate senders of RA messages and stores this information in order to validate senders of subsequent RA messages. For example, an interface that is in the learning state and receives RA messages sent from legitimate sources will dynamically transition to the forwarding state. While the interface is in forwarding state, all RA messages received on that interface that can be validated against the configured policy are forwarded.</p> <p>You can override the dynamic state transitions by requesting the forwarding state on an interface. If you issue the request for the forwarding state on an interface, the interface will remain in forwarding state until either the learning or blocking state is requested on that interface.</p>
Options	interface <i>interface-name</i> —Initiate the forwarding state on the specified interface.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateful IPv6 Router Advertisement Guard on page 514
Output Fields	This command produces no output.

request access-security router-advertisement-guard-learn interface

Syntax	<code>request access-security router-advertisement-guard-learn interface (<i>interface-name</i>) duration <i>seconds</i> (forward block)</code>
Release Information	Command introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Command introduced in Junos OS Release 16.1 for EX Series switches.
Description	<p>Request the learning state on an interface or range of interfaces for stateful IPv6 Router Advertisement (RA) guard. Stateful RA guard learns about legitimate senders of RA messages and stores this information in order to validate senders of subsequent RA messages. For example, an interface that is in the learning state and receives RA messages sent from legitimate sources dynamically transitions to the forwarding state after the learning period ends. While the interface is in forwarding state, all RA messages received on that interface that can be validated against the configured policy are forwarded.</p> <p>Before you can request learning on an interface, you must enable RA guard at the <code>[edit forwarding-options access-security router-advertisement-guard]</code> hierarchy level and configure the stateful option. When you enable stateful RA guard, the default state is Off. An interface in the Off state operates as if RA guard is not available. The learning state can be initiated only by configuring the request access-security router-advertisement-guard-learn command.</p> <p>When you request the learning state, you must configure the duration of the learning period in seconds. This is the amount of time the interface will remain in the learning state before it transitions to another state. RA messages that are received during the learning period can be either forwarded or blocked. Configure the forward option to forward RA messages during the learning period, or configure the block option to block RA messages during the learning period.</p>
Options	<p>interface <i>interface-name</i>—Initiate the learning state on the specified interface.</p> <p>duration <i>seconds</i>—Configure the duration of the learning state in seconds. When the learning period ends, the state dynamically transitions to either the forwarding state or the blocking state.</p> <p>forward—Configure the interface to forward RA messages received during the learning period.</p> <p>block—Configure the interface to block RA messages received during the learning period.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Stateful IPv6 Router Advertisement Guard on page 514

Output Fields This command produces no output.

request ipsec switch

Syntax	<code>request ipsec switch (interface <es-fpc/pic/port> security-associations <sa-name>)</code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series, PTX Series, and T Series routers and EX Series switches only) Manually switch from the primary to the backup encryption services interface, or switch from the primary to the backup IP Security (IPsec) tunnel.
Options	interface <es-fpc/pic/port> —Switch to the backup encryption interface. security-associations <sa-name> —Switch to the backup tunnel.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>show ipsec redundancy</i>
List of Sample Output	request ipsec switch security-associations on page 1108
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request ipsec switch security-associations

```
user@host> request ipsec switch security-associations sa-private
```


request security certificate enroll (Signed)

Syntax `request security certificate enroll filename filename subject subject
alternative-subject alternative-subject certification-authority certification-authority encoding
(binary | pem) key-file key-file domain-name domain-name`

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (Encryption interface on M Series and T Series routers and EX Series switches only)
Obtain a signed certificate from a certificate authority (CA). The signed certificate validates the CA and the owner of the certificate. The results are saved in a specified file to the `/var/etc/ikecert` directory.



NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard. The `request security key-pair` command is deprecated and not available with Junos in FIPS mode because it generates RSA and DSA keys with sizes of 512 and 1024 bits that are not compliant with the NIST SP 800-131A standard.

Options `filename filename`—File that stores the certificate.

`subject subject`—Distinguished name (**dn**), which consists of a set of components—for example, an organization (**o**), an organization unit (**ou**), a country (**c**), and a locality (**l**).

`alternative-subject alternative-subject`—Tunnel source address.

`certification-authority certification-authority`—Name of the certificate authority profile in the configuration.

`encoding (binary | pem)`—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default format is binary.

`key-file key-file`—File containing a local private key.

`domain-name domain-name`—Fully qualified domain name.

Required Privilege Level maintenance

List of Sample Output `request security certificate enroll filename subject alternative-subject
certification-authority key-file domain-name (Signed) on page 1110`

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

`request security certificate enroll filename subject alternative-subject certification-authority key-file
domain-name (Signed)`

```
user@host> request security certificate enroll filename host.crt subject c=uk,o=london  
alternative-subject 10.50.1.4 certification-authority verisign key-file host-1.prv domain-name  
host.example.com
```

```
CA name: example.com CA file: ca_verisign  
local pub/private key pair: host.prv  
subject: c=uk,o=london domain name: host.example.com  
alternative subject: 10.50.1.4  
Encoding: binary  
Certificate enrollment has started. To view the status of your enrollment, check  
the key management process (kmd) log file at /var/log/kmd. <-----
```

request security certificate enroll (Unsigned)

Syntax	<code>request security certificate enroll filename <i>filename</i> ca-file <i>ca-file</i> ca-name <i>ca-name</i> encoding (binary pem) url <i>url</i></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a certificate from a certificate authority (CA). The results are saved in a specified file to the <code>/var/etc/ikecert</code> directory.
Options	filename <i>filename</i> —File that stores the public key certificate. ca-file <i>ca-file</i> —Name of the certificate authority profile in the configuration. ca-name <i>ca-name</i> —Name of the certificate authority. encoding (binary pem) —File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default value is binary . url <i>url</i> —Certificate authority URL.
Required Privilege Level	maintenance
List of Sample Output	request security certificate enroll filename ca-file ca-name url (Unsigned) on page 1111
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security certificate enroll filename ca-file ca-name url (Unsigned)

```

user@host> request security certificate enroll filename ca_verisign ca-file verisign ca-name
example.com urlxyzcompany URL
http://<verisign ca-name xyzcompany url>/cgi-bin/pkiclient.exe CA name: example.com
CA file: verisign Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check
the key management process (kmd) log file at /var/log/kmd. <-----

```

request security key-pair

Syntax `request security key-pair filename`
 `<size key-size>`
 `<type (rsa | dsa)>`

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (Encryption interface on M Series and T Series routers and EX Series switches only)
 Generate a public and private key pair for a digital certificate.



NOTE: The `request security-certificates` command is deprecated and are not available with Junos in FIPS mode because security certificates are not compliant with the NIST SP 800-131A standard.

Options *filename*—Name of a file in which to store the key pair.

size *key-size*—(Optional) Key size, in bits. The key size can be **512**, **1024**, or **2048**. The default value is **1024**.

type—(Optional) Algorithm used to encrypt the key:

- **rsa**—RSA algorithm. This is the default.
- **dsa**—Digital signature algorithm with Secure Hash Algorithm (SHA).

Required Privilege Level maintenance

List of Sample Output [request security key-pair on page 1112](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security key-pair

```
user@host> request security key-pair security-key-file
```

request security pki ca-certificate enroll

Syntax	<code>request security pki ca-certificate enroll ca-profile <i>ca-profile-name</i></code>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Request a digital certificate from a certificate authority (CA) online by using the Simple Certificate Enrollment Protocol (SCEP).
Options	<code>ca-profile <i>ca-profile-name</i></code> —CA profile name.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • clear security pki ca-certificate on page 1096 • show security pki ca-certificate on page 1260
List of Sample Output	request security pki ca-certificate enroll on page 1113
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate enroll

```

user@host> request security pki ca-certificate enroll ca-profile entrust
Received following certificates:
Certificate: C=us, O=juniper, CN=First Officer
Fingerprint: 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
Certificate: C=us, O=juniper, CN=First Officer
Fingerprint: bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
Certificate: C=us, O=juniper
Fingerprint: 00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
Do you want to load the above CA certificate ? [yes,no] (no) yes

```

request security pki ca-certificate load

Syntax	<code>request security pki ca-certificate load ca-profile <i>ca-profile-name</i> filename <i>path/filename</i></code>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Manually load a certificate authority (CA) digital certificate from a specified location.
Options	ca-profile <i>ca-profile-name</i> —Load the specified CA profile. filename <i>path/filename</i> —Directory location and filename of the CA digital certificate.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• clear security pki ca-certificate on page 1096• show security pki ca-certificate on page 1260
List of Sample Output	request security pki ca-certificate load on page 1114
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate load

```
user@host> request security pki ca-certificate load ca-profile ca-private filename pki-file
```

request security pki ca-certificate verify

Syntax	<code>request security pki ca-certificate verify ca-profile <i>ca-profile-name</i></code>
Release Information	Command introduced in Junos OS Release 8.5.
Description	Verify the digital certificate installed for the specified certificate authority (CA).
Options	ca-profile <i>ca-profile-name</i> —Name of the local digital certificate identifier.
Required Privilege Level	maintenance
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

You receive the following response before the certificate revocation list (CRL) is downloaded:

```
request security pki ca-certificate verify ca-profile ca1 (CRL not downloaded)
user@host> request security pki ca-certificate verify ca-profile ca1
```

```
CA certificate ca1: CRL verification in progress. Please check the PKId debug
logs for completion status
```

request security pki crt load

Syntax	<code>request security pki crt load ca-profile <i>ca-profile-name</i> filename <i>path/filename</i></code>
Release Information	Command introduced in Junos OS Release 8.1.
Description	Manually install a certificate revocation list (CRL) on the router from a specified location.
Options	<code>ca-profile <i>ca-profile-name</i></code> —Load the specified certificate authority (CA) profile. <code>filename <i>path/filename</i></code> —Directory location and filename of the CRL.
Required Privilege Level	maintenance
List of Sample Output	request security pki crt load on page 1116
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki crt load

```
user@host> request security pki crt load ca-profile ca-private filename pki-file
```


request security pki generate-certificate-request

Syntax	<pre>request security pki generate-certificate-request certificate-id <i>certificate-id-name</i> domain-name <i>domain-name</i> subject <i>subject-distinguished-name</i> <email <i>email-address</i>> <filename (<i>path</i> <i>terminal</i>)> <ip-address <i>ip-address</i>></pre>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Manually generate a local digital certificate request in the Public-Key Cryptography Standards #10 (PKCS-10) format.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.</p> <p>subject <i>subject-distinguished-name</i>—Distinguished name format that contains the common name, department, company name, state, and country:</p> <ul style="list-style-type: none"> • CN—Common name • OU—Organizational unit name • O—Organization name • ST—State • C—Country <p>email <i>email-address</i>—(Optional) E-mail address of the certificate holder.</p> <p>filename (<i>path</i> <i>terminal</i>)—(Optional) Location where the local digital certificate request should be placed or the login terminal.</p> <p>ip-address <i>ip-address</i>—(Optional) IP address of the router.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • clear security pki certificate-request on page 1071 • show security pki certificate-request on page 1264
List of Sample Output	request security pki generate-certificate-request on page 1118

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-certificate-request

```
user@host> request security pki generate-certificate-request certificate-id local-entrust2
domain-name router2.example.net filename entrust-req2 subject cn=router2.example.net
```

```
Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHxLmp1bm1wZXIubmVOMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFk1Qws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8E1wTJ1kmIt2cB3yifB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8o0Xyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjA0BGNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBc2rq1v5S0QXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH406gQ3G
3iH0Zfz4xMIBpJYuGd1dkqgvcdH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteo1ZCiZ70f09Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

request security pki generate-key-pair

Syntax	<code>request security pki generate-key-pair certificate-id <i>certificate-id-name</i> <size (512 1024 2048)></code>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Generate a Public Key Infrastructure (PKI) public and private key pair for a local digital certificate.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>size—(Optional) Key pair size. The key pair size can be 512, 1024, or 2048 bits.</p>
Required Privilege Level	maintenance
List of Sample Output	request security pki generate-key-pair on page 1119
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-key-pair

```
user@host> request security pki generate-key-pair certificate-id billy size 2048
Generated key pair billy, key size 2048 bits
```

request security pki local-certificate enroll

Syntax	<pre>request security pki local-certificate enroll ca-profile <i>ca-profile-name</i> certificate-id <i>certificate-id-name</i> challenge-password <i>password</i> domain-name <i>domain-name</i> subject <i>subject-distinguished-name</i> <email <i>email-address</i>> <ip-address <i>ip-address</i>></pre>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Request that a certificate authority (CA) enroll and install a local digital certificate online by using the Simple Certificate Enrollment Protocol (SCEP).
Options	<p>ca-profile <i>ca-profile-name</i>—CA profile name.</p> <p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>challenge-password <i>password</i>—Password set by the administrator and normally obtained from the SCEP enrollment webpage of the CA. The password is 16 characters in length.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.</p> <p>subject <i>subject-distinguished-name</i>—Distinguished name format that contains the common name, department, company name, state, and country:</p> <ul style="list-style-type: none">• CN—Common name• OU—Organizational unit name• O—Organization name• ST—State• C—Country <p>email <i>email-address</i>—(Optional) E-mail address of the certificate holder.</p> <p>ip-address <i>ip-address</i>—(Optional) IP address of the router.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• show security pki local-certificate on page 1270

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> request security pki local-certificate enroll certificate-id r3-entrust-scep ca-profile
entrust domain-name router3.example.net subject "CN=router3,OU=Engineering,O=juniper,C=US"
challenge-password 123
```

Certificate enrollment has started. To view the status of your enrollment, check the public key infrastructure log (pkid) log file at /var/log/pkid. Please save the challenge-password for revoking this certificate in future. Note that this password is not stored on the router.

request security pki local-certificate generate-self-signed

Syntax	<code>request security pki local-certificate generate-self-signed certificate-id <i>certificate-id-name</i> domain-name <i>domain-name</i> ip-address <i>ip-address</i> email <i>email-address</i> subject <i>subject-distinguished-name</i></code>
Release Information	Command introduced in Junos OS Release 9.1.
Description	Manually generate a self-signed certificate for the given distinguished name.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.</p> <p>email <i>email-address</i>—E-mail address of the certificate holder.</p> <p>ip-address <i>ip-address</i>—IP address of the router.</p> <p>subject <i>subject-distinguished-name</i>—Distinguished name format that contains the common name, department, company name, state, and country:</p> <ul style="list-style-type: none">• CN—Common name• OU—Organizational unit name• O—Organization name• ST—State• C—Country
Required Privilege Level	<p>maintenance</p> <p>security</p>
Related Documentation	<ul style="list-style-type: none">• <i>Requesting for and Installing a Digital Certificates on Your Router</i>
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> request security pki local-certificate generate-self-signed certificate-id self-cert  
subject cn=abc domain-name example.net email user1@example.net  
Self-signed certificate generated and loaded successfully
```

request security pki local-certificate load

Syntax	<code>request security pki local-certificate load certificate-id <i>certificate-id-name</i> filename <i>path</i></code>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Manually load a local digital certificate from a specified location.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the public/private key pair mapped to the local digital certificate.</p> <p>filename <i>path/filename</i>—Directory location and filename of the local digital certificate provided by the CA.</p>
Required Privilege Level	maintenance
List of Sample Output	request security pki local-certificate load on page 1123
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki local-certificate load

```

user@host> request security pki local-certificate load filename /tmp/router2-cert certificate-id
local-entrust2
Local certificate local-entrust2 loaded successfully

```

request security pki local-certificate verify

Syntax	<code>request security pki local-certificate verify certificate-id <i>certificate-id-name</i></code>
Release Information	Command introduced in Junos OS Release 8.5.
Description	Verify the validity of the local digital certificate identifier.
Options	certificate-id <i>certificate-id-name</i> —Display the specified certificate identifier name.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• show security pki local-certificate on page 1270
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

You receive the following response before the certificate revocation list (CRL) is downloaded:

```
request security pki local-certificate verify certificate-id bme1 (not downloaded)
user@host> request security pki local-certificate verify certificate-id bme1
```

```
Local certificate bme1: CRL verification in progress. Please check the PKId debug
logs for completion status
```

You receive the following response after the certificate revocation list (CRL) is downloaded:

```
request security pki local-certificate verify certificate bme1 (downloaded)
user@host> request security pki local-certificate verify certificate-id bme1
```

```
Local certificate bme1 verification success
```

request system certificate add

Syntax	<code>request system certificate add (<i>filename</i> terminal)</code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 11.1 for the QFX Series.
Description	(Encryption interface on M Series and T Series routers, PTX Series, and QFX Series switches only) Add a certificate provided by the Juniper Networks certificate authority (CA).
Options	<i>filename</i> —Filename (URL, local, or remote). terminal —Use login terminal.
Required Privilege Level	maintenance
List of Sample Output	request system certificate add terminal on page 1125
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system certificate add terminal

```
user@host> request system certificate add terminal
```

show access-security router-advertisement state

Syntax	show access-security router-advertisement state <interface <i>interface-name</i>>
Release Information	Command introduced in Junos OS Release 15.1X53-D55 for EX3400 switches. Command introduced in Junos OS Release 16.1 for EX Series switches.
Description	Display the IPv6 Router Advertisement (RA) guard state information. Stateful RA guard enables the switch to learn about the sources of RA messages for a certain period of time. When the learning period ends, the switch has a record of which interfaces are attached to links with valid IPv6 routers. If there is no valid IPv6 router attached to the interface, the switch dynamically transitions the interface from the learning state into the blocking state. Subsequent RA messages received after the transition to blocking state are dropped. If there is a valid IPv6 router attached to the interface, the interface transitions to the forwarding state, and subsequent RA messages that can be validated against the configured policy are forwarded.
Options	interface <i>interface-name</i> —(Optional) Display the RA guard entries for the specified interface.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show access-security router-advertisement statistics on page 1128
List of Sample Output	show access-security router-advertisement state on page 1127
Output Fields	Table 41 on page 1126 lists the output fields for the show access-security router-advertisement state command. Output fields are listed in the approximate order in which they appear.

Table 41: show access-security router-advertisement state Output Fields

Field Name	Field Description
Interface	Displays the interface on which stateful IPv6 RA guard is enabled.

Table 41: show access-security router-advertisement state Output Fields (continued)

Field Name	Field Description
State	<p>Displays one of the following states:</p> <ul style="list-style-type: none">• OFF—The interface operates as if RA guard is not available.• BLOCKED—The interface blocks ingress RA messages.• FORWARDING—The interface forwards ingress RA messages that can be validated against the configured policy.• LEARNING—The switch is actively acquiring information about the IPv6 routing device connected to the interface.• TRUSTED—The interface forwards all ingress RA messages without performing policy checks.

Sample Output

show access-security router-advertisement state

```
user@device> show access-security router-advertisement state
```

Interface	state
ge-0/0/0.0	LEARNING
ge-1/0/0.0	FORWARDING
ge-1/0/0.0	BLOCKED

show access-security router-advertisement statistics

Syntax `show access-security router-advertisement statistics
<interface interface-name>`

Release Information Command introduced in Junos OS Release 15.1X53-D55 for EX3400 switches.
Command introduced in Junos OS Release 16.1 for EX Series switches.

Description Display the IPv6 Router Advertisement (RA) guard entries for received RA messages. RA guard enables a switch to examine incoming RA messages and filter them on the basis of predefined set of criteria. Once the switch has validated that the sender of the RA message is a legitimate IPv6 router, it forwards the RA message to its destination; otherwise, the RA message is dropped.

Options `interface interface-name`—(Optional) Display the RA guard entries for the specified interface.

Required Privilege Level view

Related Documentation

- [clear access-security router-advertisement statistics on page 1072](#)

List of Sample Output [show access-security router-advertisement statistics on page 1128](#)

Output Fields [Table 41 on page 1126](#) lists the output fields for the **show access-security router-advertisement statistics** command. Output fields are listed in the approximate order in which they appear.

Table 42: show access-security router-advertisement statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which the RA packet was received.	All levels
RA Packets	Total number of RA packets that were received.	All levels
RA inspection pass	Total number of RA packets that passed RA guard inspection.	All levels
RA inspection fail	Total number of RA packets that failed RA guard inspection.	All levels

Sample Output

show access-security router-advertisement statistics

```
user@device> show access-security router-advertisement statistics
```

Interface	RA Packets received	RA inspection pass	RA inspection fail
ge-0/0/7.0	3	2	1
ge-0/0/15.0	8	5	3

show arp inspection statistics

Syntax	show arp inspection statistics
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 12.1 for the QFX Series.
Description	Display ARP inspection statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear arp inspection statistics on page 1075 • Example: Configuring Port Security (non-ELS) on page 15 • Verifying That DAI Is Working Correctly on page 453
List of Sample Output	show arp inspection statistics on page 1130
Output Fields	Table 43 on page 1130 lists the output fields for the show arp inspection statistics command. Output fields are listed in the approximate order in which they appear.

Table 43: show arp inspection statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which ARP inspection has been applied.	All levels
Packets received	Total number of packets total that underwent ARP inspection.	All levels
ARP inspection pass	Total number of packets that passed ARP inspection.	All levels
ARP inspection failed	Total number of packets that failed ARP inspection.	All levels

Sample Output

show arp inspection statistics

```
user@switch> show arp inspection statistics
```

Interface	Packets received	ARP inspection pass	ARP inspection failed
-----	-----	-----	-----
ge-0/0/0	0	0	0
ge-0/0/1	0	0	0
ge-0/0/2	0	0	0
ge-0/0/3	0	0	0
ge-0/0/4	0	0	0
ge-0/0/5	0	0	0

ge-0/0/6	0	0	0
ge-0/0/7	703	701	2

show ddos-protection protocols

Syntax `show ddos-protection protocols <protocol-group (aggregate | packet-type)>`

Release Information Command introduced in Junos OS Release 11.2.
 Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
 Command introduced in Junos OS Release 14.1X53 on QFX Series switches.
 Support for Enhanced Subscriber Management added in Junos OS Release 17.3R1.

Description Display DDoS protection configuration and statistics for protocol groups or individual packet types.

Options **none**—Display information for all packet types in all protocol groups.

aggregate—(Optional) Display DDoS protection information for the aggregate policer.
 The **aggregate** option is available for all protocol groups.

packet-type—(Optional) Display DDoS protection information for the specified packet type in the protocol group. The available packet types vary by protocol group.

On QFX Series switches, only aggregate policers are available for protocol groups that are not in the following list:

- **mcast-snoop**—The following packet types are available for the **mcast-snoop** protocol group:
 - **igmp**—Control packets for IGMP snooping.
 - **mld**—Control packets for MLD snooping.
 - **pim**—Control packets for PIM snooping.
- **radius**—The following packet types are available for the **radius** protocol group:
 - **accounting**—RADIUS accounting packets.
 - **authorization**—RADIUS authorization packets.
 - **server**—RADIUS server traffic.

On MX Series routers, T4000 routers, and EX9200 switches, only aggregate policers are available for protocol groups that are not in the following list:

- **dhcipv4**—The following packet types are available for DHCPv4 traffic:
 - **ack**—DHCPACK packets.
 - **bad-packets**—DHCPv4 packets with bad formats.
 - **bootp**—DHCPBOOTP packets.
 - **decline**—DHCPDECLINE packets.

- **discover**—DHCDISCOVER packets.
- **force-renew**—DHCPFORCERENEW packets.
- **inform**—DHCPINFORM packets.
- **lease-active**—DHCPLEASEACTIVE packets.
- **lease-query**—DHCPLEASEQUERY packets.
- **lease-unassigned**—DHCPLEASEUNASSIGNED packets.
- **lease-unknown**—DHCPLEASEUNKNOWN packets.
- **nak**—DHCPNAK packets.
- **no-message-type**—DHCP packets that are missing the message type.
- **offer**—DHCOFFER packets.
- **release**—DHCPACK packets.
- **renew**—DHCPRENEW packets.
- **request**—DHCPREQUEST packets.
- **unclassified**— All unclassified packets in the protocol group.
- **dhcpv6**—The following packet types are available for DHCPv6 traffic:
 - **advertise**—ADVERTISE packets.
 - **confirm**—CONFIRM packets.
 - **decline**—DECLINE packets.
 - **information-request**—INFORMATION-REQUEST packets.
 - **leasequery**—LEASEQUERY packets.
 - **leasequery-data**—LEASEQUERY-DATA packets.
 - **leasequery-done**—LEASEQUERY-DONE packets.
 - **leasequery-reply**—LEASEQUERY-REPLY packets.
 - **rebind**—REBIND packets.
 - **reconfigure**—RECONFIGURE packets.
 - **relay-forward**—RELAY-FORWARD packets.
 - **relay-reply**—RELAY-REPLY packets.
 - **release**—RELEASE packets.
 - **renew**—RENEW packets.
 - **reply**—REPLY packets.
 - **request**—REQUEST packets.

- **solicit**—SOLICIT packets.
- **unclassified**— All unclassified packets in the protocol group.
- **filter-action**—The following packet types are available for unclassified firewall filter action packets, sent to the host because of reject terms in firewall filters:
 - **filter-v4**—Unclassified IPv4 filter action packets.
 - **filter-v6**—Unclassified IPv6 filter action packets.
 - **other**—All other unclassified filter action packets that are not IPv4 or IPv6.
- **frame-relay**—The following packet types are available for Frame Relay traffic:
 - **frf15**—Multilink frame relay FRF.15 packets.
 - **frf16**—Multilink frame relay FRF.16 packets.
- **ip-fragments**—The following packet types are available for IP fragments:
 - **first-fragment**—First IP fragment.
 - **trail-fragment**—Last IP fragment.
- **ip-options**—The following packet types are available for IP option traffic:
 - **non-v4v6**—Options packets other than IPv4/v6.
 - **router-alert**—Router alert options packets.
 - **unclassified**— All unclassified packets in the protocol group.
- **l2tp**—The following packet types are available for L2TP traffic:
 - **cdn**—Call-Disconnect-Notify message packets.
 - **hello**—Hello message packets.
 - **iccn**—Incoming-Call-Connected message packets.
 - **icrq**—Incoming-Call-Request message packets.
 - **scccn**—Start-Control-Connection-Connected message packets.
 - **sccrq**—Start-Control-Connection-Request message packets.
 - **stopccn**—Stop-Control-Connection-Notification message packets.
 - **unclassified**—All unclassified packets in the protocol group.
- **mcast-snoop**—Control traffic for multicast snooping.
 - **igmp**—Snooped IGMP traffic.
 - **pim**—Snooped PIM control traffic.
- **mlp**—The following MLP packet types are available:

- **add**—Add requests; internal MAC address learning request packets sent to the host.
- **delete**—Delete requests; internal MAC address learning request packets sent to the host.
- **lookup**—Lookup requests; internal MAC address learning request packets sent to the host.
- **unclassified**— All unclassified packets in the protocol group.
- **ndpv6**—The following packet types are available for NDPv6 traffic, except where noted, starting in 14.1R8, 14.2R8, 15.1R5, 15.1F7, and 16.1R1:
 - **invalid-hop-limit**—(Starting in 16.1R2) Invalid hop limit packets. These messages might represent crafted packets in a malicious network-based packet flood.
 - **neighbor-advertisement**—Neighbor advertisement packets. These are messages used for duplicate address detection and to test reachability of neighbors. Neighbor advertisements are sent in response to neighbor solicitation messages.
 - **neighbor-solicitation**—Neighbor solicitation packets. These are messages used for duplicate address detection and to test reachability of neighbors.
 - **redirect**—Redirect packets.
 - **router-advertisement**—Router advertisement packets. These are messages sent to announce the presence of the router, advertise prefixes, assist in address configuration, and share other link information such as MTU size and hop limit. The IPv6 nodes on the link can use this information to configure themselves with an IPv6 address and routing information such as the default gateway.
 - **router-solicitation**—Router solicitation packets. These are messages sent by IPv6 nodes when they come online to solicit immediate router advertisements from the router.
- **ppp**—The following PPP packet types are available:
 - **authentication**—PPP authentication protocol packets.
 - **echo-rep**—LCP echo reply packets.
 - **echo-req**—LCP echo request packets.
 - **ipcp**—IP Control Protocol packets.
 - **ipv6cp**—IPv6 Control Protocol packets.
 - **isis**—IS-IS packets.
 - **lcp**—Link Control Protocol packets.
 - **mlppp-lcp**—MLPPP LCP packets.
 - **mplscp**—MPLS Control Protocol packets.
 - **unclassified**— All unclassified packets in the protocol group.
- **pppoe**—The following PPPoE packet types are available:

- **padi**—PADI packets.
- **padm**—PADM packets.
- **padn**—PADN packets.
- **pado**—PADO packets.
- **padr**—PADR packets.
- **pads**—PADS packets.
- **padt**—PADT packets.
- **radius**—The following RADIUS packet types are available:
 - **accounting**—RADIUS accounting packets.
 - **authorization**—RADIUS authorization packets.
 - **server**—RADIUS server traffic.
 - **unclassified**— All unclassified packets in the protocol group.
- **re-services**—The following packet type is available for Routing Engine-based HTTP redirect IPv4 traffic:
 - **captive-portal**—Routing Engine-based captive portal content delivery packets.
- **re-services-v6**—The following packet type is available for Routing Engine-based HTTP redirect IPv6 traffic:
 - **captive-portal**—Routing Engine-based captive portal content delivery packets.
- **resolve**—The following packet types are available for unclassified resolve packets, which are sent to the host because of a traffic request resolve action:
 - **mcast-v4**—Unclassified IPv4 multicast resolve packets.
 - **mcast-v6**—Unclassified IPv6 multicast resolve packets.
 - **ucast-v4**—Unclassified IPv4 unicast resolve packets.
 - **ucast-v6**—Unclassified IPv6 unicast resolve packets.
 - **other**—All other unclassified resolve packets.
- **sample**—The following sample packet types are available:
 - **host**—Host packets.
 - **pfe**—Packet Forwarding Engine packets.
 - **syslog**—System log message packets.
 - **tap**—TAP packets.
- **tcp-flags**—The following TCP-flagged packet types are available:
 - **established**—TCP packets with ACK or RST flags set.
 - **initial**—TCP packets with SYN flag set and ACK flag not set.

- **unclassified**—TCP packets with flags set any other way than the established and initial packets.
- **unclassified**—The following unclassified packet types are available:
 - **control-layer2**—Unclassified layer 2 control packets.
 - **control-v4**—Unclassified IPv4 control packets.
 - **control-v6**—Unclassified IPv6 control packets.
 - **fw-host**—Unclassified send-to-host firewall packets.
 - **host-route-v4**—Unclassified IPv4 routing protocol and host packets in traffic sent to the router local interface address.
 - **host-route-v6**—Unclassified IPv6 routing protocol and host packets in traffic sent to the router local interface address.
 - **other**—All unclassified packets that do not belong to another type.
- **virtual-chassis**—The following packet types are available for virtual chassis packets:
 - **control-low**—Low-priority control packets.
 - **control-high**—High-priority control packets.
 - **unclassified**— All unclassified packets in the protocol group.
 - **vc-packets**—All exception packets on the virtual chassis link.
 - **vc-ttl-errors**—Virtual chassis TTL error packets.

protocol-group—(Optional) Display DDoS protection information for a protocol group. [Table 44 on page 1137](#) lists the protocol groups and the platforms they are supported on.

Table 44: Supported Protocol Groups

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX Series Switches
all-fiber-channel-enode	Fiber channel ENode traffic	—	X
amtv4	IPv4 AMT traffic	X	—
amtv6	IPv6 AMT traffic	X	—
ancp	ANCP traffic	X	—
ancpv6	ANCPv6 traffic	X	—
arp	ARP traffic	X	X
arp-snoop	ARP snooping traffic	—	X

Table 44: Supported Protocol Groups (continued)

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX Series Switches
atm	ATM traffic	X	—
bfd	Single-hop BFD traffic	X	X
bfdv6	BFDv6 traffic	X	X
bgp	BGP traffic	X	X
bgpv6	BGPv6 traffic	X	—
bridge-control	Bridge Control traffic	—	X
control	Control traffic	X	—
demux-autosense	Demux autosensing traffic	X	—
dhcpv4	DHCPv4 traffic	X	—
dhcpv6	DHCPv6 traffic	X	—
dhcpv4v6	DHCPv4 and DHCPv6 traffic	—	X
diameter	Diameter and Gx-Plus traffic	X	X
dns	DNS traffic	X	X
dtcp	DTCP traffic	X	X
dynamic-vlan	Dynamic VLAN exception traffic	X	—
egpv6	EGPv6 traffic	X	X
eoam	EOAM traffic	X	—
esmc	ESMC traffic	X	—
ethernet-tcc	TCC-encapsulated Ethernet traffic	—	X
fab-probe	Fab out probe packets	X	—
filter-action	IPv4 and IPv6 firewall filter action packets sent to the host because of reject terms in firewall filters	X	—

Table 44: Supported Protocol Groups (continued)

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX Series Switches
frame-relay	Frame relay traffic	X	—
ftp	FTP traffic	X	X
ftpv6	FTIPv6 traffic	X	—
garp-reply	Gratuitous ARP reply traffic	—	X
gre	GRE traffic	X	X
icmp	ICMP traffic	X	X
igmp	IGMP traffic	X	X
igmpv4v6	IGMP and MLD traffic	X	—
igmpv6	MLD traffic	X	—
inline-ka	Inline service interfaces keepalive traffic	X	—
inline-svcs	Inline services traffic	X	—
ip-fragments	IP fragments traffic	X	—
ip-options	IP traffic with IP packet header options	X	X
isis	IS-IS traffic	X	X
iso-tcc	TCC-encapsulated ISO traffic	—	X
jfm	JFM traffic	X	—
l2tp	Layer 2 protocol tunneling traffic	X	X
lACP	LACP traffic	X	X
ldp	LDP traffic	X	X
ldp-hello	LDP hello packets	—	X
ldpv6	LDPv6 traffic	X	—
lldp	LLDP traffic	X	X

Table 44: Supported Protocol Groups (continued)

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX Series Switches
lmp	LMP traffic	X	X
lmpv6	LMPv6 traffic	X	—
mac-host	Layer 2 MAC send-to-host traffic	X	—
martian-address	Martian address	—	—
mcast-snoop	Control traffic for multicast snooping	X	X
mld	MLD traffic	—	X
mlp	MLP traffic	X	—
msdp	MSDP traffic	X	X
multihop-bfd	Multihop BFD traffic	—	X
mld	MLD traffic	—	X
msdpv6	MSDPv6 traffic	X	—
multicast-copy	Host copy traffic due to multicast routing	X	—
mvrp	MVRP traffic	X	—
ndpv6	NDPv6 traffic	X	X
ntp	NTP traffic	X	X
oam-cfm	OAM CFM traffic	—	X
oam-lfm	OAM LFM traffic	X	X
ospf	OSPF traffic	X	X
ospf-hello	OSPF hello packets	—	X
ospfv3v6	OSPFv3/IPv6 traffic	X	—
pfe-alive	Packet Forwarding Engine keepalive traffic	X	—

Table 44: Supported Protocol Groups (continued)

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX Series Switches
pim	PIM traffic	X	—
pim-ctrl	PIM control packets	—	X
pim-data	PIM data	—	X
pimv6	PIMv6 traffic	X	—
pmvrp	PMVRP traffic	X	—
pos	POS traffic	X	—
ppp	PPP traffic	X	—
pppoe	PPPoE traffic	X	—
proto-802-1x	802.1X traffic	—	X
ptp	PTP traffic	X	X
pvstp	PVSTP traffic	X	X
radius	RADIUS traffic	X	X
re-services	Captive portal content delivery IPv4 traffic for Routing Engine HTTP redirect	X	—
re-services-v6	Captive portal content delivery IPv6 traffic for Routing Engine HTTP redirect	X	—
redirect	Traffic that triggers ICMP redirects	X	—
reject	Packets rejected by a next-hop forwarding decision	X	X
rejectv6	IPv6 packets rejected by a next-hop forwarding decision	X	—
resolve	Unclassified IPv4 and IPv6 resolve packets sent to the host because of a traffic request resolve action	X	X
rip	RIP traffic	X	X

Table 44: Supported Protocol Groups (continued)

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX Series Switches
ripv6	RIPv6 traffic	X	—
rsvp	RSVP traffic	X	X
rsvppv6	RSVPPv6 traffic	X	—
snmp	SNMP traffic	X	X
snmpv6	SNMPv6 traffic	X	—
ssh	SSH traffic	X	X
sshv6	SSHv6 traffic	X	—
stp	STP traffic	X	X
syslog	System log messages UDP traffic on port 6333 for the Routing Engine syslog server	X	—
tacacs	TACACS+ traffic	--	X
tcp-flags	Traffic with TCP flags	X	—
telnet	Telnet traffic	X	X
telnetv6	Telnetv6 traffic	X	—
ttl	Time to Live packets	X	X
tunnel-fragment	Tunnel fragments traffic	X	—
tunnel-ka	Tunnel keepalive traffic	X	—
unclassified	Unclassified traffic	X	—
virtual-chassis	Virtual chassis traffic	X	—
vrrp	VRRP traffic	X	X
vrrpv6	VRRPv6 traffic	X	—

Required Privilege Level [view](#)

- Related Documentation**
- [clear ddos-protection protocols on page 1077](#)
 - [show ddos-protection protocols culprit-flows on page 990](#)
 - [show ddos-protection protocols flow-detection on page 997](#)
 - [show ddos-protection protocols parameters on page 1153](#)
 - [show ddos-protection protocols statistics on page 1160](#)
 - [show ddos-protection protocols violations on page 1171](#)

- List of Sample Output**
- [show ddos-protection protocols on page 1148](#)
 - [show ddos-protection protocols \(Specific Packet Type with Flow Detection Disabled\) on page 1150](#)
 - [show ddos-protection protocols \(Specific Packet Type with Flow Detection Enabled and Automatic\) on page 1151](#)
 - [show ddos-protection protocols \(Specific Packet Type with Bandwidth Violation\) on page 1151](#)

- Output Fields** Table 45 on page 1143 lists the output fields for the **show ddos-protection protocols** command. Output fields are listed in the approximate order in which they appear.

Table 45: show ddos-protection protocols Output Fields

Field Name	Field Description
Packet types	Number of packet types
Modified	Number of packets for which policer values have been modified from the default.
Received traffic	Number of traffic flows received.
Currently violated	Number of flows that are currently violating the flow bandwidth limit.
Currently tracked flows	Number of active flows that are being tracked as culprit flows by flow detection.
Total detected flows	Total number of culprit flows that have been detected, including those that have recovered or timed out.
Protocol Group	Name of protocol group.
Packet type	Name of packet type in protocol group.
Bandwidth	Bandwidth policer value; number of packets per second that is allowed before a violation is declared.
Burst	Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared.

Table 45: show ddos-protection protocols Output Fields (continued)

Field Name	Field Description
Priority	Priority of the packet type for individual packet policers that enables more important traffic to pass through in the event of traffic congestion: low , medium , or high . Lower priority packets can be dropped when insufficient bandwidth is available.
Recover time	Time that must pass since the last violation before the traffic flow is considered to have recovered from the attack. A notification is generated when the timer expires.
Enabled	<p>State of the policer:</p> <ul style="list-style-type: none"> • Yes—The policer is enabled on both the Routing Engine and the FPC (line card). This is the default state. • No—The policer is disabled on both the Routing Engine and the FPC by global configuration. It is not disabled by the packet type level configuration. • No*—The policer is disabled on both the Routing Engine and the FPC. The asterisk (*) indicates that one or both of these instances is disabled at the packet type level; it may also be disabled globally. • Partial—The policer is disabled on either the Routing Engine or the FPC, but not both. It is disabled by global configuration. It is not disabled by the packet type level configuration. • Partial*—The policer is disabled on either the Routing Engine or the FPC, but not both. The asterisk (*) indicates that the instance is disabled by the packet type level configuration; it may also be disabled globally. <p>Disabling can occur globally for all packet types at the [edit system ddos-protection global] hierarchy level, for a specific packet type at the [edit system ddos-protection protocols protocol-group (aggregate packet-type)] hierarchy level, or at both levels.</p>
Bypass aggregate	<p>State of the bypass aggregate configuration:</p> <ul style="list-style-type: none"> • Yes—The aggregate policer is bypassed. • No—The aggregate policer is enforced. <p>This field appears only for individual policers.</p>

Table 45: show ddos-protection protocols Output Fields (continued)

Field Name	Field Description
Flow detection configuration	<p>State of flow detection configured on the router:</p> <ul style="list-style-type: none"> Detection mode—Mode of operation for suspicious flow detection: automatic, off, or on. Log flows—State of automatic logging of suspicious traffic flows: on (Yes) or off (No). Timeout flows—State of culprit flow timeout behavior: flow is suppressed for a configured timeout period (Yes) or flow is suppressed until it is no longer in violation (No). Detect time—Time in seconds that must pass before a suspicious flow that has exceeded the bandwidth allowed for the packet type is considered to be a culprit flow. Recover time—Time in seconds that must pass before a culprit flow is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation. Timeout time—Time in seconds that a culprit flow is suppressed, if timeouts have been enabled. Flow aggregation level configuration—Flow detection mode, flow control mode, and flow bandwidth for traffic at each of the traffic flow aggregation levels: subscriber, logical interface, and physical interface. <ul style="list-style-type: none"> Detection mode—State of flow detection: automatic, off, or on. Control mode—Mode of controlling culprit traffic: dropped, kept, or policed back to within the allowed bandwidth. Flow rate—Bandwidth allowed for the control traffic in packets per second.
System-wide information	<p>The following information collected for the router:</p> <ul style="list-style-type: none"> A message indicates whether the policer has been violated. No. of FPCs currently receiving excess traffic—Number of cards that are currently in violation of a policer. No. of FPCs that have received excess traffic—Number of cards that have at some point been in violation of a policer. Violation first detected at—Timestamp of the first violation. Violation last seen at—Timestamp of the last observed violation. Duration of violation—Length of the violation. Number of violations—Number of times the violation has occurred. Received—Number of packets received at all card slots and the Routing Engine. Dropped—Number of packets dropped regardless of where they were dropped. Arrival rate—Current traffic rate for packets arriving from all cards and at the Routing Engine. Max arrival rate—Highest traffic rate for packets arriving from all cards and at the Routing Engine.

Table 45: show ddos-protection protocols Output Fields (continued)

Field Name	Field Description
Routing Engine information	<p>The following information collected for the Routing Engine:</p> <ul style="list-style-type: none"> • Bandwidth—Maximum number of packets per second that is allowed. • Burst—Maximum number of packets that is allowed in a burst. • State of the policer: <ul style="list-style-type: none"> • enabled—The Routing Engine policer is enabled. This is the default state. • disabled—The Routing Engine policer is disabled globally. It is not disabled by the packet type level configuration. • disabled*—The Routing Engine policer is disabled by the packet type level configuration; it may also be disabled globally. • A message indicates whether the policer has been violated; the policer might be passed at the individual cards, but the combined rate of packets arriving at the Routing Engine can exceed the configured policer value. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at the Routing Engine from all cards. • Dropped—Number of packets dropped at the Routing Engine; includes packets dropped by the aggregate policer and by individual protocol policers. • Arrival rate—Current traffic rate for packets arriving at the Routing Engine from all cards. • Max arrival rate—Highest traffic rate for packets arriving at the Routing Engine from all cards. • Dropped by aggregate policer—Number of packets dropped by the aggregate policer. • Dropped by individual policers—Number of packets dropped by individual policer.

Table 45: show ddos-protection protocols Output Fields (continued)

Field Name	Field Description
FPC slot information	<p>The following information collected for the card in the indicated slot:</p> <ul style="list-style-type: none"> • Bandwidth—Bandwidth scaling percentage and the number of packets per second that is allowed before a violation is declared. • Burst—Burst scaling percentage and the maximum number of packets that is allowed in a burst before a violation is declared. • State of the policer: <ul style="list-style-type: none"> • enabled—The FPC policer is enabled. This is the default state. • disabled—The FPC policer is disabled globally. It is not disabled by the packet type level configuration. • disabled*—The FPC policer is disabled by the packet type level configuration; it may also be disabled globally. • A message indicates whether the policer has been violated. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received on the line card. • Dropped—Number of packets dropped at the line card; includes packets dropped by the aggregate policer and by individual protocol policers. • Arrival rate—Current traffic rate for packets arriving at the line card. • Max arrival rate—Highest traffic rate for packets arriving at the line card. • Dropped by this policer—Number of packets dropped by the individual policer. • Dropped by aggregate policer—Number of packets dropped by the aggregate policer. <p>NOTE: On MX Series routers with built-in MPCs—the MX5, MX10, MX40, MX80, and MX104 routers—this field actually displays information for tfeb0 because these routers have no Flexible PIC Concentrator (FPC) slots. Instead, the Packet Forwarding Engine has two “pseudo” FPCs (FPC 0 and FPC1).</p>
Bypass aggr.	<p>State of the bypass aggregate configuration:</p> <ul style="list-style-type: none"> • Yes—The aggregate policer configuration is bypassed. • No—The aggregate policer configuration is enforced. <p>Dashes indicate that the bypass aggregate configuration is not available; this is possible only for aggregate policers.</p>
FPC Mod	<p>Indicates whether configuration has changed from the default for any line cards.</p> <ul style="list-style-type: none"> • No—The default configuration has not changed from the default for the packet type. • Yes—The default configuration has changed from the default for the packet type
Op mode	<p>Mode of operation for suspicious flow detection for the packet type: always-on (on), (auto), or disabled (off).</p>

Table 45: show ddos-protection protocols Output Fields (continued)

Field Name	Field Description
Policer BW (pps)	Bandwidth policer value; number of packets per second that is allowed before a violation is declared.
Aggr level Op:Fc:Bwidth (pps)	Flow operation mode, flow control mode, and flow bandwidth for traffic of the packet type at each traffic flow aggregation level: subscriber (sub), logical interface (ifl), and physical interface (ifd).
Log flow	State of automatic logging of suspicious traffic flows for the packet type: on (Yes) or off (No).
Time out	State of culprit flow timeout behavior for the packet type: flow is suppressed or monitored for a configured timeout period (Yes) or flow is suppressed or monitored until it is no longer in violation (No).

Sample Output

show ddos-protection protocols

```
user@host> show ddos-protection protocols
```

```
Packet types: 190, Modified: 0, Received traffic: 12, Currently violated: 3
Currently tracked flows: 0, Total detected flows: 0
* = User configured value
```

```
Protocol Group: IPv4-Unclassified
```

```
Packet type: aggregate (Aggregate for unclassified host-bound IPv4 traffic)
```

```
Aggregate policer configuration:
```

```
Bandwidth:      2000 pps
Burst:          10000 packets
Recover time:   300 seconds
Enabled:        Yes
```

```
Flow detection configuration:
```

```
Detection mode: Automatic   Detect time: 3 seconds
Log flows:      No          Recover time: 60 seconds
Timeout flows: No          Timeout time: 300 seconds
```

```
Flow aggregation level configuration:
```

Aggregation level	Detection mode	Control mode	Flow rate
Subscriber	Automatic	Drop	10 pps
Logical interface	Automatic	Drop	10 pps
Physical interface	Automatic	Drop	2000 pps

```
System-wide information:
```

```
Aggregate bandwidth is never violated
Received: 0          Arrival rate: 0 pps
Dropped: 0          Max arrival rate: 0 pps
```

```
Routing Engine information:
```

```
Bandwidth: 2000 pps, Burst: 10000 packets, enabled
Aggregate policer is never violated
Received: 0          Arrival rate: 0 pps
Dropped: 0          Max arrival rate: 0 pps
Dropped by individual policers: 0
```

```
FPC slot 1 information:
```

```
Bandwidth: 100% (2000 pps), Burst: 100% (10000 packets), enabled
```



```

Aggregate policer is never violated
Received: 0                      Arrival rate: 0 pps
Dropped: 0                      Max arrival rate: 0 pps
    Dropped by individual policers: 0
    Dropped by flow suppression: 0

...

Protocol Group: PPPoE

Packet type: aggregate (Aggregate for all PPPoE control traffic)
Aggregate policer configuration:
    Bandwidth: 2000 pps
    Burst: 2000 packets
    Recover time: 300 seconds
    Enabled: Yes
Flow detection configuration:
    Detection mode: Automatic Detect time: 3 seconds
    Log flows: No Recover time: 60 seconds
    Timeout flows: No Timeout time: 300 seconds
Flow aggregation level configuration:
    Aggregation level Detection mode Control mode Flow rate
    Subscriber Automatic Drop 10 pps
    Logical interface Automatic Drop 10 pps
    Physical interface Automatic Drop 2000 pps
System-wide information:
    Aggregate bandwidth is never violated
    Received: 0                      Arrival rate: 0 pps
    Dropped: 0                      Max arrival rate: 0 pps
Routing Engine information:
    Bandwidth: 2000 pps, Burst: 2000 packets, enabled
    Aggregate policer is never violated
    Received: 0                      Arrival rate: 0 pps
    Dropped: 0                      Max arrival rate: 0 pps
        Dropped by individual policers: 0
FPC slot 1 information:
    Bandwidth: 100% (2000 pps), Burst: 100% (2000 packets), enabled
    Aggregate policer is never violated
    Received: 0                      Arrival rate: 0 pps
    Dropped: 0                      Max arrival rate: 0 pps
        Dropped by individual policers: 0
        Dropped by flow suppression: 0

Packet type: padi (PPPoE PADI)
Individual policer configuration:
    Bandwidth: 500 pps
    Burst: 500 packets
    Priority: Low
    Recover time: 300 seconds
    Enabled: Yes
    Bypass aggregate: No
Flow detection configuration:
    Detection mode: Automatic Detect time: 3 seconds
    Log flows: No Recover time: 60 seconds
    Timeout flows: No Timeout time: 300 seconds
Flow aggregation level configuration:
    Aggregation level Detection mode Control mode Flow rate
    Subscriber Automatic Drop 10 pps
    Logical interface Automatic Drop 10 pps
    Physical interface Automatic Drop 500 pps

```

```

System-wide information:
  Bandwidth is never violated
  Received: 0                      Arrival rate: 0 pps
  Dropped: 0                      Max arrival rate: 0 pps
Routing Engine information:
  Bandwidth: 500 pps, Burst: 500 packets, enabled
  Policer is never violated
  Received: 0                      Arrival rate: 0 pps
  Dropped: 0                      Max arrival rate: 0 pps
  Dropped by aggregate policer: 0
FPC slot 1 information:
  Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
  Policer is never violated
  Received: 0                      Arrival rate: 0 pps
  Dropped: 0                      Max arrival rate: 0 pps
  Dropped by aggregate policer: 0
  Dropped by flow suppression: 0
...

```

show ddos-protection protocols (Specific Packet Type with Flow Detection Disabled)

```
user@host> show ddos-protection protocols pppoe padi
```

```

Currently tracked flows: 0, Total detected flows: 0
* = User configured value

```

```
Protocol Group: PPPoE
```

```
Packet type: padi (PPPoE PADI)
```

```
Individual policer configuration:
```

```

  Bandwidth: 500 pps
  Burst: 500 packets
  Priority: Low
  Recover time: 300 seconds
  Enabled: Yes
  Bypass aggregate: No

```

```
Flow detection configuration:
```

```

Detection mode: Off*      Detect time: 3 seconds
  Log flows: No              Recover time: 60 seconds
  Timeout flows: No          Timeout time: 300 seconds

```

```
Flow aggregation level configuration:
```

Aggregation level	Detection mode	Control mode	Flow rate
Subscriber	Automatic	Drop	10 pps
Logical interface	Automatic	Drop	10 pps
Physical interface	Automatic	Drop	500 pps

```
System-wide information:
```

```

  Bandwidth is never violated
  Received: 0                      Arrival rate: 0 pps
  Dropped: 0                      Max arrival rate: 0 pps

```

```
Routing Engine information:
```

```

  Bandwidth: 500 pps, Burst: 500 packets, enabled
  Policer is never violated
  Received: 0                      Arrival rate: 0 pps
  Dropped: 0                      Max arrival rate: 0 pps
  Dropped by aggregate policer: 0

```

```
FPC slot 1 information:
```

```

  Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
  Policer is never violated
  Received: 0                      Arrival rate: 0 pps
  Dropped: 0                      Max arrival rate: 0 pps

```

```
Dropped by aggregate policer: 0
Dropped by flow suppression: 0
```

show ddos-protection protocols (Specific Packet Type with Flow Detection Enabled and Automatic)

```
user@host> show ddos-protection protocols pppoe padi
```

```
Currently tracked flows: 0, Total detected flows: 0
* = User configured value
```

```
Protocol Group: PPPoE
```

```
Packet type: padi (PPPoE PADI)
```

```
Individual policer configuration:
```

```
Bandwidth:      500 pps
Burst:          500 packets
Priority:        Low
Recover time:   300 seconds
Enabled:        Yes
Bypass aggregate: No
```

```
Flow detection configuration:
```

```
Detection mode: Automatic Detect time: 3 seconds
Log flows:      No          Recover time: 60 seconds
Timeout flows: No          Timeout time: 300 seconds
```

```
Flow aggregation level configuration:
```

Aggregation level	Detection mode	Control mode	Flow rate
Subscriber	Automatic	Drop	10 pps
Logical interface	Automatic	Drop	10 pps
Physical interface	Automatic	Drop	500 pps

```
System-wide information:
```

```
Bandwidth is never violated
Received: 0          Arrival rate: 0 pps
Dropped: 0          Max arrival rate: 0 pps
```

```
Routing Engine information:
```

```
Bandwidth: 500 pps, Burst: 500 packets, enabled
Policer is never violated
Received: 0          Arrival rate: 0 pps
Dropped: 0          Max arrival rate: 0 pps
Dropped by aggregate policer: 0
```

```
FPC slot 1 information:
```

```
Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
Policer is never violated
Received: 0          Arrival rate: 0 pps
Dropped: 0          Max arrival rate: 0 pps
Dropped by aggregate policer: 0
Dropped by flow suppression: 0
```

show ddos-protection protocols (Specific Packet Type with Bandwidth Violation)

```
user@host> show ddos-protection protocols bfd
```

```
Packet types: 1, Modified: 0, Received traffic: 1, Currently violated: 1
Currently tracked flows: 1, Total detected flows: 1
* = User configured value
```

```
Protocol Group: BFD
```

```
Packet type: aggregate (Aggregate for all bfd traffic)
```

```
Aggregate policer configuration:
```

```

Bandwidth:      20000 pps
Burst:          20000 packets
Recover time:   300 seconds
Enabled:        Yes
Flow detection configuration:
Detection mode: Automatic Detect time: 3 seconds
Log flows:      No          Recover time: 60 seconds
Timeout flows:  No          Timeout time: 300 seconds
Flow aggregation level configuration:
Aggregation level Detection mode Control mode Flow rate
Subscriber         Automatic      Drop        10 pps
Logical interface  Automatic      Drop        10 pps
Physical interface Automatic      Drop        20000 pps
System-wide information:
Aggregate bandwidth is being violated!
No. of FPCs currently receiving excess traffic: 1
No. of FPCs that have received excess traffic: 1
Violation first detected at: 2012-10-24 23:40:20 EDT
Violation last seen at:     2012-10-25 10:25:48 EDT
Duration of violation: 10:45:28 Number of violations: 1
Received: 1173471731          Arrival rate: 30304 pps
Dropped:  399135607           Max arrival rate: 30331 pps
Flow counts:
Aggregation level Current Total detected
Subscriber         1         1
Total              1         1
Routing Engine information:
Bandwidth: 20000 pps, Burst: 20000 packets, enabled
Aggregate policer is never violated
Received: 366831604          Arrival rate: 0 pps
Dropped:  0                  Max arrival rate: 9522 pps
Dropped by individual policers: 0
FPC slot 1 information:
Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled
Aggregate policer is currently being violated!
Violation first detected at: 2012-10-24 23:40:21 EDT
Violation last seen at:     2012-10-25 10:25:48 EDT
Duration of violation: 10:45:27 Number of violations: 1
Received: 1173471731          Arrival rate: 30304 pps
Dropped:  399135607           Max arrival rate: 30331 pps
Dropped by individual policers: 0
Dropped by aggregate policer: 398854530
Dropped by flow suppression: 281077
Flow counts:
Aggregation level Current Total detected State
Subscriber         1         1 Active
Logical-interface  0         0 Active
Physical-interface 0         0 Active
Total              1         1

```

show ddos-protection protocols parameters

Syntax	show ddos-protection protocols <protocol-group> parameters <brief detail terse>
Release Information	<p>Command introduced in Junos OS Release 11.2.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX Series switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 14.1X53 on QFX Series switches.</p>
Description	Display DDoS protection configuration information for all protocol groups or for a particular protocol group.
Options	<p>none—Display information for all protocol groups.</p> <p>brief detail terse—(Optional) Display the specified level of output.</p> <ul style="list-style-type: none"> • brief—Display basic function information. • detail—Add information to the brief output; it is identical to the output displayed when you choose no option. The brief and detail options display information for all protocol groups, which can be a long list. • terse—Display the same level of information as the brief option but only for active protocol groups—groups that show traffic in the Received (packets) column. <p>protocol-group—(Optional) Display information for a particular protocol group. See show ddos-protection protocols for a list of available groups.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear ddos-protection protocols on page 1077 • show ddos-protection protocols on page 1132 • show ddos-protection protocols culprit-flows on page 990 • show ddos-protection protocols flow-detection on page 997 • show ddos-protection protocols statistics on page 1160 • show ddos-protection protocols violations on page 1171
List of Sample Output	<p>show ddos-protection protocols parameters on page 1155</p> <p>show ddos-protection protocols parameters brief on page 1156</p> <p>show ddos-protection protocols dhcpv4 parameters brief on page 1157</p> <p>show ddos-protection protocols dhcpv4 parameters terse on page 1158</p> <p>show ddos-protection protocols dhcpv4 parameters on page 1158</p>

Output Fields Table 46 on page 1154 lists the output fields for the **show ddos-protection protocols parameters** command. Output fields are listed in the approximate order in which they appear.

Table 46: show ddos-protection protocols parameters Output Fields

Field Name	Field Description	Level of Output
Protocol Group	Name of protocol group.	All levels
Packet type	Name of packet type in protocol group.	All levels
Bandwidth	Bandwidth policer value; number of packets per second that is allowed before a violation is declared. In the brief output, an asterisk indicates the value has been modified from the default.	All levels
Burst	Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared. In the brief output, an asterisk indicates the value has been modified from the default.	All levels
Priority	Priority of the packet type in the event of traffic congestion: low , medium , or high . Lower priority packets can be dropped when insufficient bandwidth is available. In the brief output, an asterisk indicates the value has been modified from the default.	All levels
Recover time	Time that must pass since the last violation before the traffic flow is considered to have recovered from the attack. A notification is generated when the timer expires. In the brief output, an asterisk indicates the value has been modified from the default.	All levels
Enabled	State of the policer, enabled (Yes) or disabled (No).	detail none
Bypass aggregate	State of the bypass aggregate configuration: <ul style="list-style-type: none">• Yes—The aggregate policer is bypassed.• No—The aggregate policer is enforced. This field appears only for individual policers.	detail none
FPC slot information	The following configuration information for the card in the indicated slot: <ul style="list-style-type: none">• Bandwidth—Bandwidth scale and the number of packets per second that is allowed before a violation is declared• Burst—Burst scale and the maximum number of packets that is allowed in a burst before a violation is declared• enabled or disabled—State of the line card policer	detail none

Table 46: *show ddos-protection protocols parameters Output Fields (continued)*

Field Name	Field Description	Level of Output
Number of policers modified	Number of policers that have been changed from the default configuration. An asterisk by a particular value indicates that value has been modified.	brief terse
Policer Enabled	State of the policer, enabled (Yes), disabled (No), or partially disabled (part.); part. indicates that only some of the policer instances are disabled for the policer.	brief terse
Bypass aggr.	State of the bypass aggregate configuration: <ul style="list-style-type: none"> • Yes—The aggregate policer is bypassed. • No—The aggregate policer is enforced. Dashes indicate that the bypass aggregate configuration is not available; this is possible only for aggregate policers.	brief terse
FPC Mod	Indicates whether configuration has changed from the default for any line cards. <ul style="list-style-type: none"> • No—The default configuration has not changed from the default for the packet type. • Yes—The default configuration has changed from the default for the packet type 	brief terse

Sample Output

show ddos-protection protocols parameters

```

user@host> show ddos-protection protocols parameters

Protocol Group: IPv4-Unclassified

  Packet type: aggregate (Aggregate for unclassified host-bound IPv4 traffic)
  Aggregate policer configuration:
    Bandwidth:      20000 pps
    Burst:          20000 packets
    Priority:        medium
    Recover time:   300 seconds
    Enabled:        Yes
  FPC slot 1 information:
    Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled

Protocol Group: IPv6-Unclassified

  Packet type: aggregate (Aggregate for unclassified host-bound IPv6 traffic)
  Aggregate policer configuration:
    Bandwidth:      20000 pps
    Burst:          20000 packets
    Priority:        medium
    Recover time:   300 seconds
    Enabled:        Yes
  FPC slot 1 information:
    Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled

...

```

Protocol Group: PPPoE

Packet type: aggregate (Aggregate for all PPPoE control traffic)

Aggregate policer configuration:

Bandwidth: 800 pps
 Burst: 2000 packets
 Priority: medium
 Recover time: 300 seconds
 Enabled: Yes

FPC slot 1 information:

Bandwidth: 100% (800 pps), Burst: 100% (2000 packets), enabled

Packet type: padi (PPPoE PADI)

Individual policer configuration:

Bandwidth: 500 pps
 Burst: 500 packets
 Priority: low
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: No

FPC slot 1 information:

Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled

Packet type: pado (PPPoE PADO)

Individual policer configuration:

Bandwidth: 0 pps
 Burst: 0 packets
 Priority: low
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: No

FPC slot 1 information:

Bandwidth: 100% (0 pps), Burst: 100% (0 packets), enabled

Packet type: padr (PPPoE PADR)

Individual policer configuration:

Bandwidth: 500 pps
 Burst: 500 packets
 Priority: medium
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: No

FPC slot 1 information:

Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled

show ddos-protection protocols parameters brief

user@host> show ddos-protection protocols parameters brief

Number of policers modified: 3

Protocol group	Packet type	Bandwidth (pps)	Burst (pkts)	Priority	Recover time(sec)	Policer enabled	Bypass aggr.	FPC mod
ipv4-uncls	aggregate	20000	20000	medium	300	yes	--	no
ipv6-uncls	aggregate	20000	20000	medium	300	yes	--	no
dynvlan	aggregate	1000	500	low	300	yes	--	no
ppp	aggregate	16000	16000	medium	300	yes	--	no
ppp	unclass	1000	500	low	300	yes	no	no
ppp	lcp	12000	12000	low	300	yes	no	no
ppp	auth	2000	2000	medium	300	yes	no	no
ppp	ipcp	2000	2000	high	300	yes	no	no

ppp	ipv6cp	2000	2000	high	300	yes	no	no
ppp	mplscp	2000	2000	high	300	yes	no	no
ppp	isis	2000	2000	high	300	yes	no	no
pppoe	aggregate	800*	2000	medium	300	part.*	--	no
pppoe	padi	500	500	low	300	part.	no	no
pppoe	pado	0	0	low	300	part.	no	no
pppoe	padr	500	500	medium	300	part.	no	no
pppoe	pads	0	0	low	300	part.	no	no
pppoe	padt	1000	1000	high	300	part.	no	no
pppoe	padm	0	0	low	300	part.	no	no
pppoe	padn	0	0	low	300	part.	no	no
dhcpv4	aggregate	669*	5000	medium	300	yes	--	no
dhcpv4	unclass..	300	150	low	300	yes	no	no
dhcpv4	discover	100*	500	low	300	yes	no	no
dhcpv4	offer	1000	1000	low	300	yes	no	no
dhcpv4	request	1000	1000	medium	300	yes	no	no
dhcpv4	decline	500	500	low	300	yes	no	no
dhcpv4	ack	500	500	medium	300	yes	no	no
dhcpv4	nak	500	500	low	300	yes	no	no
dhcpv4	release	2000	2000	high	300	yes	no	no
dhcpv4	inform	500	500	low	300	yes	no	no
dhcpv4	renew	2000	2000	high	300	yes	no	no
dhcpv4	forcerenew	2000	2000	high	300	yes	no	no
dhcpv4	leasequery	2000	2000	high	300	yes	no	no
dhcpv4	leaseuna..	2000	2000	high	300	yes	no	no
dhcpv4	leaseunk..	2000	2000	high	300	yes	no	no
dhcpv4	leaseact..	2000	2000	high	300	yes	no	no
dhcpv4	bootp	300	300	low	300	yes	no	no
dhcpv4	no-msgtype	0	0	low	300	yes	no	no
dhcpv4	bad-pack..	0	0	low	300	yes	no	no
...								
icmp	aggregate	20000	20000	high	300	yes	--	no
igmp	aggregate	20000	20000	high	300	yes	--	no
ospf	aggregate	20000	20000	high	300	yes	--	no
rsvp	aggregate	20000	20000	high	300	yes	--	no
pim	aggregate	20000	20000	high	300	yes	--	no
rip	aggregate	20000	20000	high	300	yes	--	no
ptp	aggregate	20000	20000	high	300	yes	--	no
bfd	aggregate	20000	20000	high	300	yes	--	no
lmp	aggregate	20000	20000	high	300	yes	--	no
ldp	aggregate	20000	20000	high	300	yes	--	no
msdp	aggregate	20000	20000	high	300	yes	--	no
bgp	aggregate	20000	20000	low	300	yes	--	no
vrrp	aggregate	20000	20000	high	300	yes	--	no
telnet	aggregate	20000	20000	low	300	yes	--	no
ftp	aggregate	20000	20000	low	300	yes	--	no
ssh	aggregate	20000	20000	low	300	yes	--	no
snmp	aggregate	20000	20000	low	300	yes	--	no
ancp	aggregate	20000	20000	low	300	yes	--	no
...								

show ddos-protection protocols dhcpv4 parameters brief

```
user@host> show ddos-protection protocols dhcpv4 parameters brief
```

```
Number of policers modified: 2
```

Protocol	Packet	Bandwidth	Burst	Priority	Recover	Policer	Bypass	FPC
----------	--------	-----------	-------	----------	---------	---------	--------	-----

group	type	(pps)	(pkts)		time(sec)	enabled	aggr.	mod
dhcpv4	aggregate	669*	5000	medium	300	yes	--	no
dhcpv4	unclass..	300	150	low	300	yes	no	no
dhcpv4	discover	100*	500	low	300	yes	no	no
dhcpv4	offer	1000	1000	low	300	yes	no	no
dhcpv4	request	1000	1000	medium	300	yes	no	no
dhcpv4	decline	500	500	low	300	yes	no	no
dhcpv4	ack	500	500	medium	300	yes	no	no
dhcpv4	nak	500	500	low	300	yes	no	no
dhcpv4	release	2000	2000	high	300	yes	no	no
dhcpv4	inform	500	500	low	300	yes	no	no
dhcpv4	renew	2000	2000	high	300	yes	no	no
dhcpv4	forcerenew	2000	2000	high	300	yes	no	no
dhcpv4	leasequery	2000	2000	high	300	yes	no	no
dhcpv4	leaseuna..	2000	2000	high	300	yes	no	no
dhcpv4	leaseunk..	2000	2000	high	300	yes	no	no
dhcpv4	leaseact..	2000	2000	high	300	yes	no	no
dhcpv4	bootp	300	300	low	300	yes	no	no
dhcpv4	no-msgtype	0	0	low	300	yes	no	no
dhcpv4	bad-pack..	0	0	low	300	yes	no	no

show ddos-protection protocols dhcpv4 parameters terse

```
user@host> show ddos-protection protocols dhcpv4 parameters terse
```

Number of policers modified: 2

Protocol	Packet	Bandwidth	Burst	Priority	Recover	Policer	Bypass	FPC
group	type	(pps)	(pkts)		time(sec)	enabled	aggr.	mod
dhcpv4	aggregate	669*	5000	medium	300	yes	--	no
dhcpv4	discover	100*	500	low	300	yes	no	no

show ddos-protection protocols dhcpv4 parameters

```
user@host> show ddos-protection protocols dhcpv4 parameters
```

Protocol Group: DHCPv4

Packet type: aggregate (aggregate for all DHCPv4 traffic)

Aggregate policer configuration:

Bandwidth: 669 pps
 Burst: 5000 packets
 Priority: medium
 Recover time: 300 seconds
 Enabled: Yes

FPC slot 1 information:

Bandwidth: 100% (669 pps), Burst: 100% (5000 packets), enabled

Packet type: unclassified (Unclassified DHCPv4 traffic)

Individual policer configuration:

Bandwidth: 300 pps
 Burst: 150 packets
 Priority: low
 Recover time: 300 seconds
 Enabled: Yes

Bypass aggregate: No

FPC slot 1 information:

Bandwidth: 100% (300 pps), Burst: 100% (150 packets), enabled

Packet type: discover (DHCPv4 DHCPDISCOVER)

```
Individual policer configuration:
  Bandwidth:      100 pps
  Burst:          500 packets
  Priority:        low
  Recover time:   300 seconds
  Enabled:        Yes
  Bypass aggregate: No
FPC slot 1 information:
  Bandwidth: 100% (100 pps), Burst: 100% (500 packets), enabled

Packet type: offer (DHCPv4 DHCPOFFER)
Individual policer configuration:
  Bandwidth:      1000 pps
  Burst:          1000 packets
  Priority:        low
  Recover time:   300 seconds
  Enabled:        Yes
  Bypass aggregate: No
FPC slot 1 information:
  Bandwidth: 100% (1000 pps), Burst: 100% (1000 packets), enabled

Packet type: request (DHCPv4 DHCPREQUEST)
Individual policer configuration:
  Bandwidth:      1000 pps
  Burst:          1000 packets
  Priority:        medium
  Recover time:   300 seconds
  Enabled:        Yes
  Bypass aggregate: No
FPC slot 1 information:
  Bandwidth: 100% (1000 pps), Burst: 100% (1000 packets), enabled

...
```

show ddos-protection protocols statistics

Syntax `show ddos-protection protocols <protocol-group> statistics
<brief | detail | terse>`

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Command introduced in Junos OS Release 14.1X53 on QFX Series switches.

Description Display traffic statistics and DDoS policer violation statistics for all protocol groups or for a particular protocol group.



NOTE: DDoS protection policers act on the system's traffic queues. The QFX5100 and QFX5200 lines of switches manage traffic for more protocols than the number of queues, so the system often must map more than one protocol to the same queue. When traffic for one protocol shares a queue with other protocols and violates DDoS protection policer limits, this command reports a violation on that queue for all mapped protocols because the system doesn't distinguish which protocol's traffic specifically caused the violation. You can use what you know about the types of traffic flowing through your network to identify which of the reported protocols actually triggered the violation.

Options **none**—Display information for all protocol groups.

brief | detail | terse—(Optional) Display the specified level of output.

- **brief**—Display basic function information.
- **detail**—Add information to the **brief** output; it is identical to the output displayed when you choose no option. The **brief** and **detail** options display information for all protocol groups, which can be a long list.
- **terse**—Display the same level of information as the **brief** option but only for active protocol groups—groups that show traffic in the **Received (packets)** column.

protocol-group—(Optional) Display information for a particular protocol group. See [show ddos-protection protocols](#) for a list of available groups.

Required Privilege Level view

- Related Documentation**
- [clear ddos-protection protocols on page 1077](#)
 - [show ddos-protection protocols on page 1132](#)
 - [show ddos-protection protocols culprit-flows on page 990](#)
 - [show ddos-protection protocols flow-detection on page 997](#)
 - [show ddos-protection protocols parameters on page 1153](#)
 - [show ddos-protection protocols violations on page 1171](#)

- List of Sample Output**
- [show ddos-protection protocols statistics on page 1163](#)
 - [show ddos-protection protocols statistics brief on page 1166](#)
 - [show ddos-protection protocols statistics terse on page 1167](#)
 - [show ddos-protection protocols pppoe statistics on page 1167](#)
 - [show ddos-protection protocols pppoe statistics brief on page 1170](#)

Output Fields Table 47 on page 1161 lists the output fields for the **show ddos-protection protocols statistics** command. Output fields are listed in the approximate order in which they appear.

Table 47: show ddos-protection protocols statistics Output Fields

Field Name	Field Description	Level of Output
Protocol Group	Name of protocol group.	All levels
Packet type	Name of packet type in protocol group.	All levels
System-wide information	<p>The following information collected for the router:</p> <ul style="list-style-type: none"> • A message indicates whether the policer has been violated. • No. of FPCs currently receiving excess traffic—Number of cards that are currently in violation of a policer. • No. of FPCs that have received excess traffic—Number of cards that have at some point been in violation of a policer. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at all card slots and the Routing Engine. • Dropped—Number of packets dropped regardless of where they were dropped. • Arrival rate—Current traffic rate for packets arriving from all cards and at the Routing Engine. • Max arrival rate—Highest traffic rate for packets arriving from all cards and at the Routing Engine. 	detail none

Table 47: show ddos-protection protocols statistics Output Fields (continued)

Field Name	Field Description	Level of Output
Routing Engine information	<p>The following information collected for the Routing Engine:</p> <ul style="list-style-type: none"> • A message indicates whether the policer has been violated; the policer might be passed at the individual cards, but the combined rate of packets arriving at the Routing Engine can exceed the configured policer value. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at the Routing Engine from all cards. • Dropped—Number of packets dropped at the Routing Engine; includes packets dropped by the aggregate policer and by individual protocol policers. • Arrival rate—Current traffic rate for packets arriving at the Routing Engine from all cards. • Max arrival rate—Highest traffic rate for packets arriving at the Routing Engine from all cards. • Dropped by aggregate policer—Number of packets dropped by the aggregate policer. • Dropped by individual policers—Number of packets dropped by individual policer. 	detail none
FPC slot information	<p>The following information collected for the card in the indicated slot:</p> <ul style="list-style-type: none"> • A message indicates whether the policer has been violated • Violation first detected at—Timestamp of the first violation • Violation last seen at—Timestamp of the last observed violation • Duration of violation—Length of the violation • Number of violations—Number of times the violation has occurred • Received—Number of packets received on the line card • Dropped—Number of packets dropped at the line card; includes packets dropped by the aggregate policer and by individual protocol policers • Arrival rate—Current traffic rate for packets arriving at the line card • Max arrival rate—Highest traffic rate for packets arriving at the line card • Dropped by this policer—Number of packets dropped by the individual policer • Dropped by aggregate policer—Number of packets dropped by the aggregate policer 	detail none
Received (packets)	Number of packets of this packet type or protocol group received at all cards and the Routing Engine.	brief terse
Dropped (packets)	Number of packets dropped for this packet type or protocol group, regardless of where the packets were dropped.	brief terse
Rate (pps)	Highest observed traffic rate for this packet type or protocol group.	brief terse
Violation counts	Number of violations of the policer bandwidth.	brief terse

Table 47: show ddos-protection protocols statistics Output Fields (continued)

Field Name	Field Description	Level of Output
State	Violation state of the packet type: <ul style="list-style-type: none"> ok—Policer has not been violated for this packet type viol—Policer has been violated for this packet type 	brief terse

Sample Output

show ddos-protection protocols statistics

```
user@host> show ddos-protection protocols statistics
```

```
Protocol Group: IPv4-Unclassified
```

```
Packet type: aggregate
```

```
System-wide information:
```

```
Aggregate bandwidth is never violated
```

```
Received: 0 Arrival rate: 0 pps
```

```
Dropped: 0 Max arrival rate: 0 pps
```

```
Routing Engine information:
```

```
Aggregate policer is never violated
```

```
Received: 0 Arrival rate: 0 pps
```

```
Dropped: 0 Max arrival rate: 0 pps
```

```
Dropped by individual policers: 0
```

```
FPC slot 1 information:
```

```
Aggregate policer is never violated
```

```
Received: 0 Arrival rate: 0 pps
```

```
Dropped: 0 Max arrival rate: 0 pps
```

```
Dropped by individual policers: 0
```

```
Protocol Group: IPv6-Unclassified
```

```
Packet type: aggregate
```

```
System-wide information:
```

```
Aggregate bandwidth is never violated
```

```
Received: 0 Arrival rate: 0 pps
```

```
Dropped: 0 Max arrival rate: 0 pps
```

```
Routing Engine information:
```

```
Aggregate policer is never violated
```

```
Received: 0 Arrival rate: 0 pps
```

```
Dropped: 0 Max arrival rate: 0 pps
```

```
Dropped by individual policers: 0
```

```
FPC slot 1 information:
```

```
Aggregate policer is never violated
```

```
Received: 0 Arrival rate: 0 pps
```

```
Dropped: 0 Max arrival rate: 0 pps
```

```
Dropped by individual policers: 0
```

```
Protocol Group: PPPoE
```

```
Packet type: aggregate
```

```
System-wide information:
```

```
Aggregate bandwidth is never violated
```

```
Received: 61961244 Arrival rate: 4000 pps
```

```
Dropped: 0 Max arrival rate: 4002 pps
```

```
Routing Engine information:
Aggregate policer is never violated
Received: 15488871      Arrival rate: 1001 pps
Dropped: 0             Max arrival rate: 1011 pps
Dropped by individual policers: 0
FPC slot 1 information:
Aggregate policer is never violated
Received: 61961244      Arrival rate: 4000 pps
Dropped: 46473017      Max arrival rate: 4002 pps
Dropped by individual policers: 46473017

Packet type: padi
System-wide information:
Bandwidth is being violated!
No. of FPCs currently receiving excess traffic: 1
No. of FPCs that have received excess traffic: 1
Violation first detected at: 2011-04-19 08:23:17 PDT
Violation last seen at: 2011-04-19 12:41:23 PDT
Duration of violation: 04:18:06 Number of violations: 1
Received: 30980622      Arrival rate: 2000 pps
Dropped: 23236505      Max arrival rate: 2001 pps
Routing Engine information:
Policer is never violated
Received: 7744433       Arrival rate: 500 pps
Dropped: 0             Max arrival rate: 505 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is currently being violated!
Violation first detected at: 2011-04-19 08:23:17 PDT
Violation last seen at: 2011-04-19 12:41:23 PDT
Duration of violation: 04:18:06 Number of violations: 1
Received: 30980622      Arrival rate: 2000 pps
Dropped: 23236505      Max arrival rate: 2001 pps
Dropped by this policer: 23236505
Dropped by aggregate policer: 0

Packet type: pado
System-wide information:
Bandwidth is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Routing Engine information:
Policer is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Dropped by aggregate policer: 0

Packet type: padr
System-wide information:
Bandwidth is being violated!
No. of FPCs currently receiving excess traffic: 1
No. of FPCs that have received excess traffic: 1
Violation first detected at: 2011-04-19 08:23:17 PDT
Violation last seen at: 2011-04-19 12:43:23 PDT
Duration of violation: 04:20:06 Number of violations: 1
```



```

Received: 31220846      Arrival rate: 2000 pps
Dropped: 23416690      Max arrival rate: 2001 pps
Routing Engine information:
Policer is never violated
Received: 7806417      Arrival rate: 499 pps
Dropped: 0             Max arrival rate: 506 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is currently being violated!
Violation first detected at: 2011-04-19 08:23:17 PDT
Violation last seen at: 2011-04-19 12:43:23 PDT
Duration of violation: 04:20:06 Number of violations: 1
Received: 31220846      Arrival rate: 2000 pps
Dropped: 23416690      Max arrival rate: 2001 pps
Dropped by this policer: 23416690
Dropped by aggregate policer: 0

Packet type: pads
System-wide information:
Bandwidth is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Routing Engine information:
Policer is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Dropped by aggregate policer: 0

Packet type: padt
System-wide information:
Bandwidth is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Routing Engine information:
Policer is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Dropped by aggregate policer: 0

Packet type: padm
System-wide information:
Bandwidth is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Routing Engine information:
Policer is never violated
Received: 0             Arrival rate: 0 pps
Dropped: 0             Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:

```

```

Policer is never violated
Received: 0          Arrival rate: 0 pps
Dropped: 0          Max arrival rate: 0 pps
Dropped by aggregate policer: 0

Packet type: padn
System-wide information:
Bandwidth is never violated
Received: 0          Arrival rate: 0 pps
Dropped: 0          Max arrival rate: 0 pps
Routing Engine information:
Policer is never violated
Received: 0          Arrival rate: 0 pps
Dropped: 0          Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is never violated
Received: 0          Arrival rate: 0 pps
Dropped: 0          Max arrival rate: 0 pps
Dropped by aggregate policer: 0

...

```

show ddos-protection protocols statistics brief

```
user@host> show ddos-protection protocols statistics brief
```

Protocol group	Packet type	Received (packets)	Dropped (packets)	Rate (pps)	Violation counts	State
ipv4-uncls	aggregate	0	0	0	0	ok
ipv6-uncls	aggregate	0	0	0	0	ok
dynvlan	aggregate	0	0	0	0	ok
ppp	aggregate	0	0	0	0	ok
ppp	unclass	0	0	0	0	ok
ppp	lcp	0	0	0	0	ok
ppp	auth	0	0	0	0	ok
ppp	ipcp	0	0	0	0	ok
ppp	ipv6cp	0	0	0	0	ok
ppp	mplscp	0	0	0	0	ok
ppp	isis	0	0	0	0	ok
pppoe	aggregate	61561238	0	4000	0	ok
pppoe	padi	30780619	23086506	2000	1	viol
pppoe	pado	0	0	0	0	ok
pppoe	padr	30780619	23086499	2000	1	viol
pppoe	pads	0	0	0	0	ok
pppoe	padt	0	0	0	0	ok
pppoe	padm	0	0	0	0	ok
pppoe	padn	0	0	0	0	ok
dhcpv4	aggregate	0	0	0	0	ok
dhcpv4	unclass..	0	0	0	0	ok
dhcpv4	discover	0	0	0	0	ok
dhcpv4	offer	0	0	0	0	ok
dhcpv4	request	0	0	0	0	ok
dhcpv4	decline	0	0	0	0	ok
dhcpv4	ack	0	0	0	0	ok
dhcpv4	nak	0	0	0	0	ok
dhcpv4	release	0	0	0	0	ok
dhcpv4	inform	0	0	0	0	ok
dhcpv4	renew	0	0	0	0	ok

dhcpv4	forcerenew	0	0	0	0	ok
dhcpv4	leasequery	0	0	0	0	ok
dhcpv4	leaseuna..	0	0	0	0	ok
dhcpv4	leaseunk..	0	0	0	0	ok
dhcpv4	leaseact..	0	0	0	0	ok
dhcpv4	bootp	0	0	0	0	ok
dhcpv4	no-msgtype	0	0	0	0	ok
dhcpv4	bad-pack..	0	0	0	0	ok
...						
icmp	aggregate	0	0	0	0	ok
igmp	aggregate	0	0	0	0	ok
ospf	aggregate	0	0	0	0	ok
rsvp	aggregate	0	0	0	0	ok
pim	aggregate	0	0	0	0	ok
rip	aggregate	0	0	0	0	ok
ptp	aggregate	0	0	0	0	ok
bfd	aggregate	0	0	0	0	ok
lmp	aggregate	0	0	0	0	ok
ldp	aggregate	0	0	0	0	ok
msdp	aggregate	0	0	0	0	ok
bgp	aggregate	0	0	0	0	ok
vrp	aggregate	0	0	0	0	ok
telnet	aggregate	0	0	0	0	ok
...						

show ddos-protection protocols statistics terse

```
user@host> show ddos-protection protocols statistics terse
```

Protocol group	Packet type	Received (packets)	Dropped (packets)	Rate (pps)	Violation counts	State
ipv4-unc1s	aggregate	241	0	0	0	ok
icmp	aggregate	20	0	0	0	ok
igmp	aggregate	55	0	0	0	ok
ospf	aggregate	956	0	0	0	ok
rsvp	aggregate	784	0	0	0	ok
ldp	aggregate	2984	0	0	0	ok
bgp	aggregate	312	0	0	0	ok
larp	aggregate	1744	0	0	0	ok
stp	aggregate	9791	0	0	0	ok
arp	aggregate	19	0	0	0	ok
pvstp	aggregate	393	0	0	0	ok
m1p	aggregate	624774	0	0	0	ok
m1p	packets	1714371	223937	0	3	ok
mcast-copy	aggregate	3018038	0	0	0	ok
igmp-snoop	aggregate	43	0	0	0	ok
fw-host	aggregate	95547	0	0	0	ok
unc1s	aggregate	10000	0	0	0	ok

show ddos-protection protocols pppoe statistics

```
user@host> show ddos-protection protocols pppoe statistics
```

```
Protocol Group: PPPoE
```

```
Packet type: aggregate
System-wide information:
  Aggregate bandwidth is never violated
  Received: 60381200          Arrival rate: 4000 pps
  Dropped: 0                  Max arrival rate: 4002 pps
Routing Engine information:
  Aggregate policer is never violated
  Received: 15095242          Arrival rate: 1001 pps
  Dropped: 0                  Max arrival rate: 1011 pps
  Dropped by individual policers: 0
FPC slot 1 information:
  Aggregate policer is never violated
  Received: 60381200          Arrival rate: 4000 pps
  Dropped: 45287921          Max arrival rate: 4002 pps
  Dropped by individual policers: 45287921
```

```
Packet type: padi
System-wide information:
  Bandwidth is being violated!
  No. of FPCs currently receiving excess traffic: 1
  No. of FPCs that have received excess traffic: 1
  Violation first detected at: 2011-04-19 08:23:17 PDT
  Violation last seen at: 2011-04-19 12:34:48 PDT
  Duration of violation: 04:11:31 Number of violations: 1
  Received: 30190600          Arrival rate: 2000 pps
  Dropped: 22643960          Max arrival rate: 2001 pps
Routing Engine information:
  Policer is never violated
  Received: 7547621           Arrival rate: 499 pps
  Dropped: 0                  Max arrival rate: 505 pps
  Dropped by aggregate policer: 0
FPC slot 1 information:
  Policer is currently being violated!
  Violation first detected at: 2011-04-19 08:23:17 PDT
  Violation last seen at: 2011-04-19 12:34:48 PDT
  Duration of violation: 04:11:31 Number of violations: 1
  Received: 30190600          Arrival rate: 2000 pps
  Dropped: 22643960          Max arrival rate: 2001 pps
  Dropped by this policer: 22643960
  Dropped by aggregate policer: 0
```

```
Packet type: pado
System-wide information:
  Bandwidth is never violated
  Received: 0                  Arrival rate: 0 pps
  Dropped: 0                  Max arrival rate: 0 pps
Routing Engine information:
  Policer is never violated
  Received: 0                  Arrival rate: 0 pps
  Dropped: 0                  Max arrival rate: 0 pps
  Dropped by aggregate policer: 0
FPC slot 1 information:
  Policer is never violated
  Received: 0                  Arrival rate: 0 pps
  Dropped: 0                  Max arrival rate: 0 pps
  Dropped by aggregate policer: 0
```

```
Packet type: padr
System-wide information:
  Bandwidth is being violated!
```

```

    No. of FPCs currently receiving excess traffic: 1
    No. of FPCs that have received excess traffic: 1
    Violation first detected at: 2011-04-19 08:23:17 PDT
    Violation last seen at:    2011-04-19 12:34:48 PDT
    Duration of violation: 04:11:31 Number of violations: 1
    Received: 30190600          Arrival rate:    2000 pps
    Dropped:  22643961          Max arrival rate: 2001 pps
Routing Engine information:
    Policer is never violated
    Received: 7547621          Arrival rate:    501 pps
    Dropped:  0                Max arrival rate: 506 pps
    Dropped by aggregate policer: 0
FPC slot 1 information:
    Policer is currently being violated!
    Violation first detected at: 2011-04-19 08:23:17 PDT
    Violation last seen at:    2011-04-19 12:34:48 PDT
    Duration of violation: 04:11:31 Number of violations: 1
    Received: 30190600          Arrival rate:    2000 pps
    Dropped:  22643961          Max arrival rate: 2001 pps
    Dropped by this policer: 22643961
    Dropped by aggregate policer: 0

Packet type: pads
System-wide information:
    Bandwidth is never violated
    Received: 0                Arrival rate:    0 pps
    Dropped:  0                Max arrival rate: 0 pps
Routing Engine information:
    Policer is never violated
    Received: 0                Arrival rate:    0 pps
    Dropped:  0                Max arrival rate: 0 pps
    Dropped by aggregate policer: 0
FPC slot 1 information:
    Policer is never violated
    Received: 0                Arrival rate:    0 pps
    Dropped:  0                Max arrival rate: 0 pps
    Dropped by aggregate policer: 0

Packet type: padt
System-wide information:
    Bandwidth is never violated
    Received: 0                Arrival rate:    0 pps
    Dropped:  0                Max arrival rate: 0 pps
Routing Engine information:
    Policer is never violated
    Received: 0                Arrival rate:    0 pps
    Dropped:  0                Max arrival rate: 0 pps
    Dropped by aggregate policer: 0
FPC slot 1 information:
    Policer is never violated
    Received: 0                Arrival rate:    0 pps
    Dropped:  0                Max arrival rate: 0 pps
    Dropped by aggregate policer: 0

Packet type: padm
System-wide information:
    Bandwidth is never violated
    Received: 0                Arrival rate:    0 pps
    Dropped:  0                Max arrival rate: 0 pps
:

```

```

Policer is never violated
Received: 0                      Arrival rate: 0 pps
Dropped: 0                      Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is never violated
Received: 0                      Arrival rate: 0 pps
Dropped: 0                      Max arrival rate: 0 pps
Dropped by aggregate policer: 0

Packet type: padn
System-wide information:
Bandwidth is never violated
Received: 0                      Arrival rate: 0 pps
Dropped: 0                      Max arrival rate: 0 pps
:
Policer is never violated
Received: 0                      Arrival rate: 0 pps
Dropped: 0                      Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is never violated
Received: 0                      Arrival rate: 0 pps
Dropped: 0                      Max arrival rate: 0 pps
Dropped by aggregate policer: 0

```

show ddos-protection protocols pppoe statistics brief

```
user@host> show ddos-protection protocols pppoe statistics brief
```

Protocol group	Packet type	Received (packets)	Dropped (packets)	Rate (pps)	Violation counts	State
pppoe	aggregate	60901227	0	4000	0	ok
pppoe	padi	30450613	22838981	2000	1	viol
pppoe	pado	0	0	0	0	ok
pppoe	padr	30450614	22838977	2000	1	viol
pppoe	pads	0	0	0	0	ok
pppoe	padt	0	0	0	0	ok
pppoe	padm	0	0	0	0	ok
pppoe	padn	0	0	0	0	ok

show ddos-protection protocols violations

Syntax `show ddos-protection protocols <protocol-group> violations`

Release Information Command introduced in Junos OS Release 11.2.
 Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
 Command introduced in Junos OS Release 14.1X53 on QFX Series switches.

Description Display information about DDoS policer violations for all protocol groups or for a particular protocol group.



NOTE: DDoS protection policers act on the system's traffic queues. The QFX5100 and QFX5200 lines of switches manage traffic for more protocols than the number of queues, so the system often must map more than one protocol to the same queue. When traffic for one protocol shares a queue with other protocols and violates DDoS protection policer limits, this command reports a violation on that queue for all mapped protocols because the system doesn't distinguish which protocol's traffic specifically caused the violation. You can use what you know about the types of traffic flowing through your network to identify which of the reported protocols actually triggered the violation.

Options `none`—Display information for all protocol groups.

`protocol-group`—(Optional) Name of a particular protocol group. See [show ddos-protection protocols](#) for a list of available groups.

Required Privilege Level view

Related Documentation

- [clear ddos-protection protocols on page 1077](#)
- [show ddos-protection protocols on page 1132](#)
- [show ddos-protection protocols culprit-flows on page 990](#)
- [show ddos-protection protocols flow-detection on page 997](#)
- [show ddos-protection protocols parameters on page 1153](#)
- [show ddos-protection protocols statistics on page 1160](#)

List of Sample Output [show ddos-protection protocols violations on page 1172](#)
[show ddos-protection protocols lldp violations on page 1172](#)

[show ddos-protection protocols pppoe violations on page 1172](#)

Output Fields [Table 48 on page 1172](#) lists the output fields for the **show ddos-protection protocols violations** command. Output fields are listed in the approximate order in which they appear.

Table 48: show ddos-protection protocols violations Output Fields

Field Name	Field Description
Number of packet types that are being violated	Number of individual policers and aggregate policers that are currently being violated
Protocol Group	Name of protocol group
Packet type	Name of packet type in protocol group
Bandwidth (pps)	Policer bandwidth
Arrival rate (pps)	Current traffic rate for packets arriving from all cards and at the Routing Engine
Peak rate (pps)	Highest traffic rate for packets arriving from all cards and at the Routing Engine
Policer bandwidth violation detected at	Timestamp of the policer violation
Detected on	Slot number of the card on which the violation was detected

Sample Output

show ddos-protection protocols violations

```
user@host> show ddos-protection protocols violations
```

```
Number of packet types that are being violated: 2
Protocol  Packet    Bandwidth  Arrival  Peak    Policer bandwidth
group     type      (pps)      rate(pps) rate(pps) violation detected at
pppoe     padi      500        2000     2001    2011-04-19 08:23:17 PDT
          Detected on: FPC-1
pppoe     padr      500        1999     2001    2011-04-19 08:23:17 PDT
          Detected on: FPC-1
```

show ddos-protection protocols lldp violations

```
user@host> show ddos-protection protocols lldp violations
```

```
Number of packet types that are being violated: 0
```

show ddos-protection protocols pppoe violations

```
user@host> show ddos-protection protocols pppoe violations
```



```
Number of packet types that are being violated: 2
Protocol  Packet      Bandwidth  Arrival  Peak    Policer bandwidth
group     type        (pps)      rate(pps) rate(pps) violation detected at
pppoe     padi        500        2000     2001    2011-04-19 08:23:17 PDT
          Detected on: FPC-1
pppoe     padr        500        1999     2001    2011-04-19 08:23:17 PDT
          Detected on: FPC-1
```

show ddos-protection statistics

Syntax	show ddos-protection statistics
Release Information	<p>Command introduced in Junos OS Release 11.2.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 14.1X53 on QFX Series switches.</p>
Description	Display DDoS protection global statistics for bandwidth violations.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear ddos-protection protocols on page 1077 • show ddos-protection protocols on page 1132 • show ddos-protection version on page 1176
List of Sample Output	show ddos-protection statistics on page 1175
Output Fields	Table 49 on page 1174 lists the output fields for the show ddos-protection statistics command. Output fields are listed in the approximate order in which they appear.

Table 49: show ddos-protection statistics Output Fields

Field Name	Field Description
Policing on routing engine	Shows whether or not policing is enabled on the Routing Engine.
Policing on FPC	Shows whether or not policing is enabled on the line card.
Flow detection	Shows whether or not flow detection is enabled.
Logging	Shows whether or not DDoS event logging is enabled.
Policer violation report rate	Shows the violation report rate as a percentage.
Flow report rate	Shows the flow report rate as a percentage.
Default flow detection mode	Flow detection and tracking mode configured at the global level for all protocol groups and packet types.

Table 49: show ddos-protection statistics Output Fields (continued)

Field Name	Field Description
Default flow level detection mode	Flow detection and tracking mode configured at the flow aggregation level for all protocol groups and packet types.
Default flow level control mode	Default behavior configured for how traffic in detected flows is controlled for all protocol groups and packet types.
Currently violated packet types	Number of packet types currently experiencing a bandwidth violation.
Packet types have seen violations	Number of packet types that have experienced a bandwidth violation since statistics were cleared.
Total violation counts	Total number of bandwidth violations.

Sample Output

show ddos-protection statistics

```
user@host> show ddos-protection statistics
```

```
DDOS protection global statistics:
  Policing on routing engine:      Yes
  Policing on FPC:                 Yes
  Flow detection:                   No
  Logging:                         Yes
  Policer violation report rate:    100
  Flow report rate:                 100
  Default flow detection mode       Automatic
  Default flow level detection mode Automatic
  Default flow level control mode   Drop
  Currently violated packet types:   2
  Packet types have seen violations: 4
  Total violation counts:            4
  Currently tracked flows:           0
  Total detected flows:              0
```

show ddos-protection version

Syntax	show ddos-protection version
Release Information	<p>Command introduced in Junos OS Release 11.2.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 14.1X53 on QFX Series switches.</p>
Description	Display the DDoS protection version and the total numbers of protocol groups and packet types that this version can be configured in this version.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear ddos-protection protocols on page 1077 • show ddos-protection protocols on page 1132 • show ddos-protection statistics on page 1174
List of Sample Output	show ddos-protection version on page 1176
Output Fields	<p>Table 50 on page 1176 lists the output fields for the show ddos-protection version command. Output fields are listed in the approximate order in which they appear.</p>

Table 50: show ddos-protection version Output Fields

Field Name	Field Description
Version	Version number of the DDoS protection code.
Total protocol groups	Number of protocol groups configured with DDoS protection.
Total tracked packet types	Number of protocol packet types configured with DDoS protection.

Sample Output

show ddos-protection version

```
user@host> show ddos-protection version
```

```
DDOS protection, Version 1.0
Total protocol groups      = 83
Total tracked packet types = 154
```

show dhcp snooping binding

Syntax	show dhcp snooping binding <interface <i>interface-name</i>> <vlan <i>vlan-name</i>>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 12.1 for the QFX Series.
Description	Display the DHCP snooping database information.
Options	interface <i>interface-name</i> —(Optional) Display the DHCP snooping database information for an interface. vlan <i>vlan-name</i> —(Optional) Display the DHCP snooping database information for a VLAN.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcp snooping binding on page 1079 • Example: Configuring Port Security (non-ELS) on page 15 • Enabling DHCP Snooping (non-ELS) on page 400
List of Sample Output	show dhcp snooping binding on page 1179
Output Fields	Table 51 on page 1178 lists the output fields for the show dhcp snooping binding command. Output fields are listed in the approximate order in which they appear.

Table 51: show dhcp snooping binding Output Fields

Field Name	Field Description	Level of Output
MAC Address	MAC address of the network device; bound to the IP address.	All levels
IP Address	IP address of the network device; bound to the MAC address.	All levels
Lease	Lease granted to the IP address.	All levels
Type	How the MAC address was acquired.	All levels
VLAN	VLAN name of the network device whose MAC address is shown.	All levels
Interface	Interface address (port).	All levels

Sample Output

show dhcp snooping binding

```
user@switch> show dhcp snooping binding
```

DHCP Snooping Information:

MAC Address	IP Address	Lease	Type	VLAN	Interface
00:00:01:00:00:03	192.0.2.0	640	dynamic	guest	ge-0/0/12.0
00:00:01:00:00:04	192.0.2.1	720	dynamic	guest	ge-0/0/12.0
00:00:01:00:00:05	192.0.2.5	800	dynamic	guest	ge-0/0/13.0

show dhcp snooping statistics

Syntax	<code>show dhcp snooping statistics</code>
Release Information	Command introduced in Junos OS Release 9.4 for EX Series switches.
Description	Display statistics for read and write operations to the DHCP snooping database.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcp snooping statistics on page 1080 • Understanding DHCP Snooping (non-ELS) on page 393
List of Sample Output	show dhcp snooping statistics on page 1180
Output Fields	Table 52 on page 1180 lists the output fields for the <code>show dhcp snooping statistics</code> command. Output fields are listed in the approximate order in which they appear.

Table 52: show dhcp snooping statistics Output Fields

Field Name	Field Description
Successful Transfers	Number of entries successfully transferred from memory to the DHCP snooping database.
Successful Reads	Number of entries successfully read from memory to the DHCP snooping database.
Successful Writes	Number of entries successfully written from memory to the DHCP snooping database.
Failed Transfers	Number of entries that failed being transferred from memory to the DHCP snooping database.
Failed Reads	Number of entries that failed being read from memory to the DHCP snooping database.
Failed Writes	Number of entries that failed being written from memory to the DHCP snooping database.

Sample Output

show dhcp snooping statistics

```
user@switch> show dhcp snooping statistics
```

```
Successful Transfers :      0   Failed Transfers :      21
Successful Reads    :      0   Failed Reads    :      0
Successful Writes   :      0   Failed Writes   :      21
```


show dhcp-security arp inspection statistics

Syntax	show dhcp-security arp inspection statistics
Release Information	Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Command introduced in Junos OS Release 14.1 for the MX Series.
Description	Display Address Resolution Protocol (ARP) inspection statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show dhcp-security binding on page 1183 • clear dhcp-security binding on page 1081 • clear interfaces statistics • Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487 • Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 497 • Port Security Features on page 3
List of Sample Output	show dhcp-security arp inspection statistics on page 1182
Output Fields	<p>Table 53 on page 1181 lists the output fields for the show dhcp-security arp inspection statistics command. Output fields are listed in the approximate order in which they appear.</p> <p>The IP source guard database table shows the untrusted access interfaces in VLANs that have been enabled for IP source guard. The entries include the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another.</p>

Table 53: show dhcp-security arp inspection statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which ARP inspection has been applied.	All levels
Packets received	Total number of packets that underwent ARP inspection.	All levels
ARP inspection pass	Total number of packets that passed ARP inspection.	All levels
ARP inspection fail	Total number of packets that failed ARP inspection.	All levels

Sample Output

show dhcp-security arp inspection statistics

```
user@device> show dhcp-security arp inspection statistics
```

Interface	Packets received	ARP inspection pass	ARP inspection fail
ge-0/0/30.0	7	7	0
ge-0/0/4.0	3	3	0
ge-0/0/6.0	72	4	68

show dhcp-security binding

Syntax	<pre>show dhcp-security binding <interface <i>interface-name</i>> <ip-address <i>ip-address</i>> <ip-source-guard <i>ip-sg-name</i>> <statistics> <vlan <i>vlan-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Command introduced in Junos OS Release 14.1 for the MX Series.</p>
Description	Display the DHCP snooping database information.
Options	<p>interface <i>interface-name</i>—(Optional) Display the DHCP snooping database information for an interface.</p> <p>ip-address <i>ip-address</i>—(Optional) Display the DHCP snooping database information for an IP address.</p> <p>vlan <i>vlan-name</i>—(Optional) Display the DHCP snooping database information for a VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show dhcp-security binding ip-source-guard on page 1186 • clear dhcp-security binding on page 1081 • Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487 • Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 497 • Port Security Features on page 3
List of Sample Output	<p>show dhcp-security binding on page 1184</p> <p>show dhcp-security binding interface on page 1184</p> <p>show dhcp-security binding ip-address on page 1185</p> <p>show dhcp-security binding vlan on page 1185</p>
Output Fields	<p>Table 54 on page 1184 lists the output fields for the show dhcp-security binding command. Output fields are listed in the approximate order in which they appear.</p>

Table 54: show dhcp-security binding Output Fields

Field Name	Field Description	Level of Output
IP Address	IP address of the network device; bound to the MAC address.	All levels
MAC address	MAC address of the network device; bound to the IP address.	All levels
VLAN	VLAN name of the network device whose MAC address is shown.	All levels
Expires	The time, in seconds, remaining before the lease of the IP address to the MAC address expires. This field is 0 for static entries.	All levels
State	Specifies whether the IP address is: <ul style="list-style-type: none"> BOUND: Leased to the MAC address for a limited period of time. STATIC: Attached to a fixed MAC address. 	All levels
Interface	Interface address (port).	All levels

Sample Output

show dhcp-security binding

```
user@device> show dhcp-security binding
```

IP address	MAC address	Vlan	Expires	State	Interface
10.1.1.10	00:10:00:20:00:01	vlan20	0	STATIC	ge-0/0/4.0
10.1.1.18	00:10:94:00:00:34	vlan20	86287	BOUND	ge-0/0/6.0
10.1.1.15	00:10:94:00:00:55	vlan20	86265	BOUND	ge-0/0/4.0
10.1.1.16	00:10:94:00:00:56	vlan20	86265	BOUND	ge-0/0/4.0
10.1.1.19	00:10:94:00:00:5b	vlan20	86287	BOUND	ge-0/0/6.0
10.1.1.20	00:10:94:00:00:5c	vlan20	86287	BOUND	ge-0/0/6.0
10.1.1.21	00:10:94:00:00:5d	vlan20	86287	BOUND	ge-0/0/6.0
10.1.1.17	00:10:94:00:00:68	vlan20	86265	BOUND	ge-0/0/4.0

show dhcp-security binding interface

```
user@device> show dhcp-security binding interface ge-0/0/6
```

IP address	MAC address	Vlan	Expires	State	Interface
10.1.1.18	00:10:94:00:00:34	vlan20	86282	BOUND	ge-0/0/6.0
10.1.1.19	00:10:94:00:00:5b	vlan20	86282	BOUND	ge-0/0/6.0
10.1.1.20	00:10:94:00:00:5c	vlan20	86282	BOUND	ge-0/0/6.0

10.1.1.21	00:10:94:00:00:5d	vlan20	86282	BOUND	ge-0/0/6.0
-----------	-------------------	--------	-------	-------	------------

show dhcp-security binding ip-address

user@device> show dhcp-security binding ip-address

IP address	MAC address	Vlan	Expires	State	Interface
10.1.1.18	00:10:94:00:00:34	vlan20	86282	BOUND	ge-0/0/6.0

show dhcp-security binding vlan

user@device> show dhcp-security binding vlan vlan20

IIP address	MAC address	Vlan	Expires	State	Interface
10.1.1.18	00:10:94:00:00:34	vlan20	86282	BOUND	ge-0/0/6.0

show dhcp-security binding ip-source-guard

Syntax	show dhcp-security binding ip-source-guard
Release Information	Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Command introduced in Junos OS Release 14.1 for the MX Series.
Description	Display IP source guard database table.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show dhcp-security binding on page 1183 • clear dhcp-security binding on page 1081 • Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 487 • Example: Configuring IP Source Guard and Dynamic ARP Inspection on a Specified Bridge Domain to Protect the Devices Against Attacks on page 497 • Port Security Features on page 3
List of Sample Output	show dhcp-security binding ip-source-guard on page 1187
Output Fields	<p>Table 55 on page 1186 lists the output fields for the show dhcp-security binding ip-source-guard command. Output fields are listed in the approximate order in which they appear.</p> <p>The IP source guard database table shows the untrusted access interfaces in VLANs that have been enabled for IP source guard. The entries include the IP addresses and MAC addresses that are bound to one another.</p>

Table 55: show dhcp-security binding ip-source-guard Output Fields

Field Name	Field Description	Level of Output
IP Address	IP address of the network device; bound to the MAC address.	All levels
MAC address	MAC address of the network device; bound to the IP address.	All levels
VLAN	VLAN name of the network device whose MAC address is shown.	All levels
Expires	The time, in seconds, remaining before the lease of the IP address to the MAC address expires.	All levels

Table 55: show dhcp-security binding ip-source-guard Output Fields (continued)

Field Name	Field Description	Level of Output
State	Specifies whether the IP address is: <ul style="list-style-type: none"> BOUND: Temporarily leased to the MAC address for a limited period of time. STATIC: Attached to a fixed MAC address. 	All levels
Interface	Interface address (port).	All levels

Sample Output

show dhcp-security binding ip-source-guard

```
user@device> show dhcp-security binding ip-source-guard
```

IP address	MAC address	Vlan	Expires	State	Interface
10.1.1.10	00:10:00:20:00:01	vlan20	0	STATIC	ge-0/0/4.0
10.1.1.18	00:10:94:00:00:34	vlan20	86276	BOUND	ge-0/0/6.0
10.1.1.15	00:10:94:00:00:55	vlan20	86254	BOUND	ge-0/0/4.0
10.1.1.16	00:10:94:00:00:56	vlan20	86254	BOUND	ge-0/0/4.0
10.1.1.19	00:10:94:00:00:5b	vlan20	86276	BOUND	ge-0/0/6.0
10.1.1.20	00:10:94:00:00:5c	vlan20	86276	BOUND	ge-0/0/6.0
10.1.1.21	00:10:94:00:00:5d	vlan20	86276	BOUND	ge-0/0/6.0
10.1.1.17	00:10:94:00:00:68	vlan20	86254	BOUND	ge-0/0/4.0

show dhcp-security ipv6 binding

Syntax	<pre>show dhcp-security ipv6 binding <interface <i>interface-name</i>> <ipv6-address <i>ipv6-address</i>> <vlan <i>vlan-name</i>></pre>
Release Information	Command introduced in Junos OS Release 13.2X51-D20 for EX Series switches. Command introduced in Junos OS Release 17.2R1 for the QFX Series.
Description	Display bindings between IPv6 addresses and MAC addresses (IP-MAC bindings) along with other DHCP lease information, also known as the DHCPv6 binding table or DHCPv6 snooping database.
Options	<p>interface <i>interface-name</i>—(Optional) Display the DHCPv6 snooping table for the specified interface.</p> <p>ipv6-address <i>ipv6-address</i>—(Optional) Display the DHCPv6 snooping table for the specified IPv6 address.</p> <p>vlan <i>vlan-name</i>—(Optional) Display the DHCPv6 snooping table for a VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show dhcp-security ipv6 statistics on page 1190• clear dhcp-security ipv6 binding on page 1082• Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 492
List of Sample Output	show dhcp-security ipv6 binding on page 1189 show dhcp-security ipv6 binding interface on page 1189
Output Fields	<p>Table 55 on page 1186 lists the output fields for the show dhcp-security ipv6 binding command. Output fields are listed in the approximate order in which they appear.</p> <p>The DHCPv6 binding table shows the untrusted access interfaces in VLANs that have been enabled for DHCPv6 snooping. The entries include the IPv6 addresses and MAC addresses that are bound to one another.</p>

Table 56: show dhcp-security ipv6 binding Output Fields

Field Name	Field Description	Level of Output
IPv6 address	IPv6 addresses of the network device; bound to the MAC address. There are two entries added for each client: one with the link-local IPv6 address, which is used by the client for DHCP transactions, and another with the IPv6 address assigned by the server. The link-local address always has the prefix fe80::/10.	All levels
MAC address	MAC address of the network device; bound to the IPv6 address.	All levels
VLAN	VLAN name of the network device whose MAC address is shown.	All levels
Expires	The time, in seconds, remaining before the lease of the IPv6 address to the MAC address expires. This field is 0 for static entries.	All levels
State	Specifies whether the IPv6 address is: <ul style="list-style-type: none"> • BOUND: Temporarily leased to the MAC address for a limited period of time. • STATIC: Attached to a fixed MAC address. 	All levels
Interface	Interface address (port).	All levels

Sample Output

show dhcp-security ipv6 binding

```
user@switch> show dhcp-security ipv6 binding
```

IPv6 address	MAC address	Vlan	Expires	State	Interface
2001:db8:fe10::	00:10:94:00:55:0b	vlan20	3456	BOUND	ge-0/0/1.0
fe80::210:94ff:fe00:1	00:10:94:00:55:0b	vlan20	3456	BOUND	ge-0/0/1.0
2001:db8:fe12::	00:10:94:00:00:34	vlan20	3456	BOUND	ge-0/0/2.0
fe80::210:94ff:fe00:2	00:10:94:00:00:34	vlan20	3456	BOUND	ge-0/0/2.0
2001:db8:fe14::	00:10:94:00:00:55	vlan20	3456	BOUND	ge-0/0/3.0
fe80::210:94ff:fe00:3	00:10:94:00:00:55	vlan20	3456	BOUND	ge-0/0/3.0

Sample Output

show dhcp-security ipv6 binding interface

```
user@switch> show dhcp-security ipv6 binding interface ge-0/0/4.0
```

IPv6 address	MAC address	Vlan	Expires	State	Interface
2001:db8:fe16::	00:10:00:20:00:01	vlan20	0	STATIC	ge-0/0/4.0
fe80::210:94ff:fe00:4	00:10:00:20:00:01	vlan20	0	STATIC	ge-0/0/4.0

show dhcp-security ipv6 statistics

Syntax	<code>show dhcp-security ipv6 statistics</code>
Release Information	Command introduced in Junos OS Release 13.2X51-D20 for EX Series switches.
Description	Display DHCPv6 statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show dhcp-security ipv6 binding on page 1188• show dhcp-security neighbor-discovery-inspection statistics on page 1193
List of Sample Output	show dhcp-security ipv6 statistics on page 1192
Output Fields	Table 57 on page 1191 lists the output fields for the <code>show dhcp-security ipv6 statistics</code> command. Output fields are listed in the approximate order in which they appear.

Table 57: show dhcp-security ipv6 statistics Output Fields

Field Name	Field Description
DHCPv6 messages	<p>Number of DHCPv6 messages exchanged.</p> <ul style="list-style-type: none"> • Total—Total number of DHCPv6 messages exchanged. • Solicit—Number of DHCPv6 messages of type Solicit. A client sends a Solicit message to locate servers. • Advertise—Number of DHCPv6 messages of type Advertise. A server sends an Advertise message, in response to a Solicit message, to indicate that it is available for DHCPv6 service. • Request—Number of DHCPv6 messages of type Request. A client sends a Request message to request configuration parameters from a server. • Reply—Number of DHCPv6 messages of type Reply. A server sends a Reply message in response to a Solicit, Request, Renew, Rebind, Confirm, Information Request, Release, or Decline message. • Confirm—Number of DHCPv6 messages of type Confirm. A client sends a Confirm message to any available server to determine whether the addresses it was assigned are still appropriate for the link to which the client is connected. • Decline—Number of DHCPv6 messages of type Decline. A client sends a Decline message to a server to indicate that one or more of the addresses assigned by the server are already in use on the link to which the client is connected. • Release—Number of DHCPv6 messages of type Release. A client sends a Release message to the server to indicate that the client will no longer use one or more of the assigned addresses. • Renew—Number of DHCPv6 messages of type Renew. A client sends a Renew message to the server to extend the lifetimes on the addresses assigned to the client by that server and to update other configuration parameters received by that server. • Rebind—Number of DHCPv6 messages of type Rebind. A client sends a Rebind message to any available server after receiving no reply to a Renew message. • Relay-forward—Number of DHCPv6 messages of type Relay-forward. A relay agent sends a Relay-forward message to relay messages to servers, either directly or through another relay agent. The received message is encapsulated in an option in the Relay-forward message. • Relay-reply—Number of DHCPv6 messages of type Relay-reply. A server sends a Relay-reply message to a relay agent containing a message that the relay agent delivers to a client. • Information-request—Number of DHCPv6 messages of type Information-request. A client sends an Information-request message to a server to request configuration parameters without the assignment of any IP addresses to the client. • Reconfigure—Number of DHCPv6 messages of type Reconfigure. A server sends a Reconfigure message to a client to inform the client that the server has new or updated configuration parameters, and that the client needs to initiate a Renew/Reply or Information-request/Reply transaction with the server in order to receive the updated information.
Packets dropped	<p>Number of packets not considered for DHCPv6 snooping because of errors.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by DHCPv6 snooping. • No configuration—Number of packets discarded because they did not have a valid configuration. • No VLAN—Number of packets discarded because they did not belong to a valid VLAN. • No interface—Number of packets discarded because they did not belong to a valid interface. • Request on trusted port—Number of packets discarded because a Request message was received on a trusted port.

Sample Output

show dhcp-security ipv6 statistics

```
user@host> show dhcp-security ipv6 statistics
```

DHCPv6 messages:

Total	32
Solicit	1
Advertise	1
Request	3
Reply	5
Confirm	1
Decline	2
Release	9
Renew	4
Rebind	2
Relay forward	1
Relay reply	1
Information request	1
Reconfigure	2

Packets dropped:

Total	0
No configuration	0
No VLAN	0
No interface	0
Request on trusted port	0

show dhcp-security neighbor-discovery-inspection statistics

Syntax	show dhcp-security neighbor-discovery-inspection statistics <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 13.2X51-D20 for EX Series switches.
Description	Display IPv6 neighbor discovery inspection statistics to determine whether there is IPv6 address spoofing on the network.
Options	interface <i>interface-name</i> —(Optional) Display neighbor discovery inspection statistics for the specified interface.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show dhcp-security ipv6 binding on page 1188 • IPv6 Neighbor Discovery Inspection on page 509 • Example: Configuring IPv6 Source Guard and Neighbor Discovery Inspection to Protect a Switch from IPv6 Address Spoofing on page 492
List of Sample Output	show dhcp-security neighbor-discovery-inspection statistics on page 1193 show dhcp-security neighbor-discovery-inspection statistics interface on page 1194
Output Fields	Table 53 on page 1181 lists the output fields for the show dhcp-security neighbor-discovery-inspection statistics command. Output fields are listed in the approximate order in which they appear.

Table 58: show dhcp-security neighbor-discovery-inspection statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which neighbor discovery inspection has been applied.	All levels
Packets received	Total number of packets that underwent neighbor discovery inspection.	All levels
ND inspection pass	Total number of packets that passed neighbor discovery inspection.	All levels
ND inspection fail	Total number of packets that failed neighbor discovery inspection.	All levels

Sample Output

show dhcp-security neighbor-discovery-inspection statistics

```
user@switch> show dhcp-security neighbor-discovery-inspection statistics
```

Interface	ND Packets received	ND inspection pass	ND inspection failed
ge-0/0/1.0	7	5	2
ge-0/0/2.0	10	10	0
ge-0/0/3.0	12	12	0

Sample Output

show dhcp-security neighbor-discovery-inspection statistics interface

```
user@switch> show dhcp-security neighbor-discovery-inspection statistics interface ge-0/0/1.0
```

Interface	ND Packets received	ND inspection pass	ND inspection failed
ge-0/0/1.0	7	5	2

show dhcpv6 snooping binding

Syntax `show dhcpv6 snooping binding`
`<interface interface-name>`
`<vlan vlan-name>`

Release Information Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Display the DHCPv6 snooping database information.

Options `interface interface-name`—(Optional) Display the DHCPv6 snooping database information for an interface.

`vlan vlan-name`—(Optional) Display the DHCPv6 snooping database information for a VLAN.

Required Privilege Level view

Related Documentation

- [clear dhcp snooping binding on page 1079](#)
- [Example: Configuring Port Security \(non-ELS\) on page 15](#)
- [Enabling DHCP Snooping \(non-ELS\) on page 400](#)

List of Sample Output [show dhcpv6 snooping binding on page 1196](#)

Output Fields [Table 51 on page 1178](#) lists the output fields for the `show dhcpv6 snooping binding` command. Output fields are listed in the approximate order in which they appear.

Table 59: show dhcp snooping binding Output Fields

Field Name	Field Description	Level of Output
MAC Address	MAC address of the network device; bound to the IP address.	All levels
IP Address	IP address of the network device; bound to the MAC address.	All levels
Lease	Lease granted to the IP address.	All levels
Type	How the MAC address was acquired.	All levels
VLAN	VLAN name of the network device whose MAC address is shown.	All levels
Interface	Interface address (port).	All levels

Sample Output

show dhcpv6 snooping binding

```
user@switch> show dhcpv6 snooping binding
```

DHCP Snooping Information:

MAC address	IP address	Lease (seconds)	Type	VLAN	Interface
00:10:94:00:00:01	2001:db8::10:10	3599992	dynamic	v1	ge-0/0/0.0
00:10:94:00:00:01	fe80::210:94ff:fe00:1	3599992	dynamic	v1	ge-0/0/0.0
00:10:94:00:00:02	2001:db8::10:11	3599992	dynamic	v1	ge-0/0/0.0
00:10:94:00:00:02	fe80::210:94ff:fe00:2	3599992	dynamic	v1	ge-0/0/0.0
00:10:94:00:00:03	2001:db8::10:12	3599992	dynamic	v1	ge-0/0/0.0
00:10:94:00:00:03	fe80::210:94ff:fe00:3	3599992	dynamic	v1	ge-0/0/0.0
00:10:94:00:00:04	2001:db8::10:13	3599992	dynamic	v1	ge-0/0/0.0
00:10:94:00:00:04	fe80::210:94ff:fe00:4	3599992	dynamic	v1	ge-0/0/0.0
00:10:94:00:00:05	2001:db8::10:14	3599992	dynamic	v1	ge-0/0/0.0
00:10:94:00:00:05	fe80::210:94ff:fe00:5	3599992	dynamic	v1	ge-0/0/0.0

show dhcpv6 snooping statistics

Syntax	<code>show dhcpv6 snooping statistics</code>
Release Information	Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Display statistics for read and write operations performed on the DHCPv6 snooping database.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcp snooping statistics on page 1080 • Understanding DHCP Snooping (non-ELS) on page 393
List of Sample Output	show dhcpv6 snooping statistics on page 1197
Output Fields	Table 52 on page 1180 lists the output fields for the show dhcpv6 snooping statistics command. Output fields are listed in the approximate order in which they appear.

Table 60: show dhcpv6 snooping statistics Output Fields

Field Name	Field Description
Successful Transfers	Number of entries successfully transferred from memory to the DHCPv6 snooping database.
Successful Reads	Number of entries successfully read from memory to the DHCPv6 snooping database.
Successful Writes	Number of entries successfully written from memory to the DHCPv6 snooping database.
Failed Transfers	Number of entries that failed being transferred from memory to the DHCPv6 snooping database.
Failed Reads	Number of entries that failed being read from memory to the DHCPv6 snooping database.
Failed Writes	Number of entries that failed being written from memory to the DHCPv6 snooping database.

Sample Output

show dhcpv6 snooping statistics

```

user@switch> show dhcpv6 snooping statistics
DHCP Snoop Persistence statistics
Successful Remote Transfers: 0      Failed Remote Transfers: 0
Successful Record Reads   : 0      Failed Record Reads   : 0
Successful Record Writes  : 0      Failed Record Writes  : 0

```

show ethernet-switching table

List of Syntax	Syntax (QFX Series, QFabric, NFX Series and EX4600) on page 1198 Syntax (EX Series) on page 1198 Syntax (EX Series, MX Series and QFX Series) on page 1198 Syntax (SRX Series) on page 1198
Syntax (QFX Series, QFabric, NFX Series and EX4600)	<pre>show ethernet-switching table <brief detail extensive summary> <interface <i>interface-name</i>> <management-vlan> <sort-by (<i>name</i> <i>tag</i>)> <vlan <i>vlan-name</i>></pre>
Syntax (EX Series)	<pre>show ethernet-switching table <brief detail extensive summary> <interface <i>interface-name</i>> <management-vlan> <persistent-mac <interface <i>interface-name</i>>> <sort-by (<i>name</i> <i>tag</i>)> <vlan <i>vlan-name</i>></pre>
Syntax (EX Series, MX Series and QFX Series)	<pre>show ethernet-switching table <brief count detail extensive summary> <<i>address</i>> <instance <i>instance-name</i>> <interface <i>interface-name</i>> isis <i>isid</i> <logical-system <i>logical-system-name</i>> <persistent-learning (interface <i>interface-name</i> mac <i>mac-address</i>)> <<i>address</i>> <vlan-id (all-vlan <i>vlan-id</i>)> <vlan-name (all <i>vlan-name</i>)></pre>
Syntax (SRX Series)	<pre>show ethernet-switching table (brief detail extensive) interface <i>interface-name</i></pre>
Release Information	<p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 9.5 for SRX Series.</p> <p>Options summary, management-vlan, and vlan <i>vlan-name</i> introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Option sort-by and field name tag introduced in Junos OS Release 10.1 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Output for private VLANs introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Option persistent-mac introduced in Junos OS Release 11.4 for EX Series switches.</p> <p>Command introduced in Junos OS Release 12.3R2.</p>

Command introduced in Junos OS Release 12.3R2 for EX Series switches.

Options **logical-system**, **persistent-learning**, and **summary** introduced in Junos OS Release 13.2X50-D10 (ELS).

Description Displays the Ethernet switching table.

(MX Series routers, EX Series switches only) Displays Layer 2 MAC address information.

Options For QFX Series, QFabric, NFX Series and EX4600:

none—(Optional) Display brief information about the Ethernet switching table.

brief | detail | extensive | summary—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display the Ethernet switching table for a specific interface.

management-vlan—(Optional) Display the Ethernet switching table for a management VLAN.

persistent-mac <interface *interface-name*>—(Optional) Display the persistent MAC addresses learned for all interfaces or a specified interface. You can use this command to view entries that you want to clear for an interface that you intentionally disabled.

sort-by (*name | tag*)—(Optional) Display VLANs in ascending order of VLAN IDs or VLAN names.

vlan *vlan-name*—(Optional) Display the Ethernet switching table for a specific VLAN.

For EX Series, MX Series and QFX Series:

none—Display all learned Layer 2 MAC address information.

brief | count | detail | extensive | summary—(Optional) Display the specified level of output.

address—(Optional) Display the specified learned Layer 2 MAC address information.

instance *instance-name*—(Optional) Display learned Layer 2 MAC addresses for the specified routing instance.

interface *interface-name*—(Optional) Display learned Layer 2 MAC addresses for the specified interface.

isid *isid*—(Optional) Display learned Layer 2 MAC addresses for the specified ISID.

logical-system *logical-system-name*—(Optional) Display Ethernet-switching statistics information for the specified logical system.

persistent-learning (interface *interface-name* | mac *mac-address*)—(Optional) Display dynamically learned MAC addresses that are retained despite device restarts and

interface failures for a specified interface, or information about a specified MAC address.

vlan-id (all-vlan | vlan-id)—(Optional) Display learned Layer 2 MAC addresses for all VLANs or for the specified VLAN.

vlan-name (all | vlan-name)—(Optional) Display learned Layer 2 MAC addresses for all VLANs or for the specified VLAN.

For SRX Series:

- **none**—(Optional) Display brief information about the Ethernet switching table.
- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **interface-name**—(Optional) Display the Ethernet switching table for a specific interface.

Additional Information When Layer 2 protocol tunneling is enabled, the tunneling MAC address 01:00:0c:cd:cd:d0 is installed in the MAC table. When the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP) is configured for Layer 2 protocol tunneling on an interface, the corresponding protocol MAC address is installed in the MAC table.

Required Privilege Level view

Related Documentation

- *Example: Setting Up Basic Bridging and a VLAN on Switches*
- *Example: Setting Up Bridging with Multiple VLANs*
- *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*
- *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
- *Example: Setting Up Q-in-Q Tunneling on EX Series Switches*
- [clear ethernet-switching table on page 1089](#)
- *show ethernet-switching mac-learning-log*

List of Sample Output

[show ethernet-switching table \(Enhanced Layer 2 Software on QFX Series, QFabric, NFX Series and EX460\) on page 1204](#)
[show ethernet-switching table \(QFX Series, QFabric, NFX Series and EX460\) on page 1205](#)
[show ethernet-switching table \(Private VLANs on QFX Series, QFabric, NFX Series and EX460\) on page 1206](#)
[show ethernet-switching table \(Junos Fusion Data Center with EVPN on QFX Series switches\) on page 1206](#)
[show ethernet-switching table brief \(QFX Series, QFabric, NFX Series and EX460\) on page 1207](#)
[show ethernet-switching table detail \(QFX Series, QFabric, NFX Series and EX460\) on page 1208](#)
[show ethernet-switching table extensive \(QFX Series, QFabric, NFX Series and EX460\) on page 1209](#)

[show ethernet-switching table interface \(QFX Series, QFabric, NFX Series and EX460\) on page 1211](#)
[show ethernet-switching table \(EX Series switches\) on page 1211](#)
[show ethernet-switching table brief \(EX Series switches\) on page 1212](#)
[show ethernet-switching table detail \(EX Series switches\) on page 1212](#)
[show ethernet-switching table extensive \(EX Series switches\) on page 1213](#)
[show ethernet-switching table persistent-mac \(EX Series switches\) on page 1213](#)
[show ethernet-switching table persistent-mac interface ge-0/0/16.0 \(EX Series switches\) on page 1214](#)
[show ethernet-switching table \(EX Series, MX Series and QFX Series\) on page 1214](#)
[show ethernet-switching table brief on page 1215](#)
[show ethernet-switching table count on page 1216](#)
[show ethernet-switching table extensive on page 1217](#)
[show ethernet-switching table detail \(SRX Series\) on page 1218](#)
[show ethernet-switching table extensive \(SRX Series\) on page 1219](#)
[show ethernet-switching table interface ge-0/0/1 \(SRX Series\) on page 1220](#)

Output Fields For QFX Series, QFabric, NFX Series and EX4600:

The following table lists the output fields for the **show ethernet-switching table** command on QFX Series, QFabric, NFX Series and EX4600. Output fields are listed in the approximate order in which they appear.

Table 61: show ethernet-switching table Output Fields

Field Name	Field Description	Level of Output
VLAN	Name of a VLAN.	All levels
MAC address	MAC address associated with the VLAN.	All levels
Type	Type of MAC address: <ul style="list-style-type: none"> static—The MAC address is manually created. learn—The MAC address is learned dynamically from a packet's source MAC address. flood—The MAC address is unknown and flooded to all members. 	All levels
Age	Time remaining before the entry ages out and is removed from the Ethernet switching table.	All levels
Interfaces	Interface associated with learned MAC addresses or with the All-members option (flood entry).	All levels
Learned	For learned entries, the time at which the entry was added to the Ethernet switching table.	detail, extensive

For EX Series switches:

The following table lists the output fields for the **show ethernet-switching table** command on EX Series switches. Output fields are listed in the approximate order in which they appear.

Table 62: show ethernet-switching table Output Fields

Field Name	Field Description	Level of Output
VLAN	The name of a VLAN.	All levels
Tag	The VLAN ID tag name or number.	extensive
MAC or MAC address	The MAC address associated with the VLAN.	All levels
Type	The type of MAC address. Values are: <ul style="list-style-type: none"> • static—The MAC address is manually created. • learn—The MAC address is learned dynamically from a packet's source MAC address. • flood—The MAC address is unknown and flooded to all members. • persistent—The learned MAC addresses that will persist across restarts of the switch or interface-down events. 	All levels except persistent-mac
Type	The type of MAC address. Values are: <ul style="list-style-type: none"> • installed—addresses that are in the Ethernet switching table. • uninstalled—addresses that could not be installed in the table or were uninstalled in an interface-down event and will be reinstalled in the table when the interface comes back up. 	persistent-mac
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.	All levels
Interfaces	Interface associated with learned MAC addresses or All-members (flood entry).	All levels
Learned	For learned entries, the time which the entry was added to the Ethernet switching table.	detail, extensive
Nexthop index	The next-hop index number.	detail, extensive
persistent-mac	installed indicates MAC addresses that are in the Ethernet switching table and uninstalled indicates MAC addresses that could not be installed in the table or were uninstalled in an interface-down event (and will be reinstalled in the table when the interface comes back up).	

For EX Series, MX Series and QFX Series:

The table describes the output fields for the **show ethernet-switching table** command on EX Series, MX Series and QFX Series. Output fields are listed in the approximate order in which they appear.

Table 63: show ethernet-switching table Output fields

Field Name	Field Description
Routing instance	Name of the routing instance.
VLAN name	Name of the VLAN.

Table 63: show ethernet-switching table Output fields (continued)

Field Name	Field Description
MAC address	MAC address or addresses learned on a logical interface.
MAC flags	Status of MAC address learning properties for each interface: <ul style="list-style-type: none"> • S—Static MAC address is configured. • D—Dynamic MAC address is configured. • L—Locally learned MAC address is configured. • SE—MAC accounting is enabled. • NM—Non-configured MAC. • R—Locally learned MAC address is configured.
Age	This field is not supported.
Logical interface	Name of the logical interface.
Active source	IP address of remote entity on which MAC address is learned.
MAC count	Number of MAC addresses learned on the specific routing instance or interface.
Learning interface	Name of the logical interface on which the MAC address was learned.
Learning VLAN	VLAN ID of the routing instance or VLAN in which the MAC address was learned.
Layer 2 flags	Debugging flags signifying that the MAC address is present in various lists.
Epoch	Spanning-tree-protocol epoch number identifying when the MAC address was learned. Used for debugging.
Sequence number	Sequence number assigned to this MAC address. Used for debugging.
Learning mask	Mask of the Packet Forwarding Engines where this MAC address was learned. Used for debugging.
IPC generation	Creation time of the logical interface when this MAC address was learned. Used for debugging.

For SRX Series:

[Table 64 on page 1203](#) lists the output fields for the **show ethernet-switching table** command. Output fields are listed in the approximate order in which they appear.

Table 64: show ethernet-switching table Output Fields

Field Name	Field Description
VLAN	The name of a VLAN.

Table 64: show ethernet-switching table Output Fields (continued)

Field Name	Field Description
MAC address	The MAC address associated with the VLAN.
Type	The type of MAC address. Values are: <ul style="list-style-type: none"> static—The MAC address is manually created. learn—The MAC address is learned dynamically from a packet's source MAC address. flood—The MAC address is unknown and flooded to all members.
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.
Interfaces	Interface associated with learned MAC addresses or All-members (flood entry).
Learned	For learned entries, the time which the entry was added to the Ethernet switching table.

Sample Output

show ethernet-switching table (Enhanced Layer 2 Software on QFX Series, QFabric, NFX Series and EX460)

```

user@switch> show ethernet-switching table

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent
static
      SE - statistics enabled, NM - non configured MAC, R - remote PE MAC,
O - ovsdb MAC)

Ethernet switching table : 2 entries, 2 learned
Routing instance : default-switch
  Vlan      MAC      MAC      Age      Logical
  name      address  flags
  vlan1     b0:c6:9a:ca:3c:01  D        -        ae1.0

  vlan1     b0:c6:9a:ca:3c:03  D        -        ae1.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent
static
      SE - statistics enabled, NM - non configured MAC, R - remote PE MAC,
O - ovsdb MAC)

Ethernet switching table : 2 entries, 2 learned
Routing instance : default-switch
  Vlan      MAC      MAC      Age      Logical
  name      address  flags
  vlan10    b0:c6:9a:ca:3c:01  D        -        ae1.0

  vlan10    b0:c6:9a:ca:3c:03  D        -        ae1.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent
static

```


SE - statistics enabled, NM - non configured MAC, R - remote PE MAC,
0 - ovssdb MAC)

Ethernet switching table : 2 entries, 2 learned

Routing instance : default-switch

Vlan name	MAC address	MAC flags	Age	Logical interface
vlan2	b0:c6:9a:ca:3c:01	D	-	ae1.0
vlan2	b0:c6:9a:ca:3c:03	D	-	ae1.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static

SE - statistics enabled, NM - non configured MAC, R - remote PE MAC,
0 - ovssdb MAC)

Ethernet switching table : 2 entries, 2 learned

Routing instance : default-switch

Vlan name	MAC address	MAC flags	Age	Logical interface
vlan3	b0:c6:9a:ca:3c:01	D	-	ae1.0
vlan3	b0:c6:9a:ca:3c:03	D	-	ae1.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static

SE - statistics enabled, NM - non configured MAC, R - remote PE MAC,
0 - ovssdb MAC)

Ethernet switching table : 2 entries, 2 learned

Routing instance : default-switch

Vlan name	MAC address	MAC flags	Age	Logical interface
vlan4	b0:c6:9a:ca:3c:01	D	-	ae1.0
vlan4	b0:c6:9a:ca:3c:03	D	-	ae1.0

show ethernet-switching table (QFX Series, QFabric, NFX Series and EX460)

user@switch> show ethernet-switching table

Ethernet-switching table: 57 entries, 17 learned

VLAN	MAC address	Type	Age	Interfaces
F2	*	Flood	-	All-members
F2	00:00:05:00:00:03	Learn	0	xe-0/0/44.0
F2	00:19:e2:50:7d:e0	Static	-	Router
Linux	*	Flood	-	All-members
Linux	00:19:e2:50:7d:e0	Static	-	Router
Linux	00:30:48:90:54:89	Learn	0	xe-0/0/47.0
T1	*	Flood	-	All-members
T1	00:00:05:00:00:01	Learn	0	xe-0/0/46.0
T1	00:00:5e:00:01:00	Static	-	Router
T1	00:19:e2:50:63:e0	Learn	0	xe-0/0/46.0
T1	00:19:e2:50:7d:e0	Static	-	Router
T10	*	Flood	-	All-members

```

T10      00:00:5e:00:01:09 Static      - Router
T10      00:19:e2:50:63:e0 Learn      0 xe-0/0/46.0
T10      00:19:e2:50:7d:e0 Static      - Router
T111     *                          Flood      - All-members
T111     00:19:e2:50:63:e0 Learn      0 xe-0/0/15.0
T111     00:19:e2:50:7d:e0 Static      - Router
T111     00:19:e2:50:ac:00 Learn      0 xe-0/0/15.0
T2       *                          Flood      - All-members
T2       00:00:5e:00:01:01 Static      - Router
T2       00:19:e2:50:63:e0 Learn      0 xe-0/0/46.0
T2       00:19:e2:50:7d:e0 Static      - Router
T3       *                          Flood      - All-members
T3       00:00:5e:00:01:02 Static      - Router
T3       00:19:e2:50:63:e0 Learn      0 xe-0/0/46.0
T3       00:19:e2:50:7d:e0 Static      - Router
T4       *                          Flood      - All-members
T4       00:00:5e:00:01:03 Static      - Router
T4       00:19:e2:50:63:e0 Learn      0 xe-0/0/46.0
[output truncated]

```

show ethernet-switching table (Private VLANs on QFX Series, QFabric, NFX Series and EX460)

```
user@switch> show ethernet-switching table
```

```

Ethernet-switching table: 10 entries, 3 learned
VLAN      MAC address      Type      Age Interfaces
pvlan     *                Flood      - All-members
pvlan     00:10:94:00:00:02 Replicated - xe-0/0/28.0
pvlan     00:10:94:00:00:35 Replicated - xe-0/0/46.0
pvlan     00:10:94:00:00:46 Replicated - xe-0/0/4.0
c2        *                Flood      - All-members
c2        00:10:94:00:00:02 Learn      0 xe-0/0/28.0
c1        *                Flood      - All-members
c1        00:10:94:00:00:46 Learn      0 xe-0/0/4.0
__pvlan_pvlan_xe-0/0/46.0__ *      Flood      - All-members
__pvlan_pvlan_xe-0/0/46.0__ 00:10:94:00:00:35 Learn      0 xe-0/0/46.0

```

show ethernet-switching table (Junos Fusion Data Center with EVPN on QFX Series switches)

```
user@switch> show ethernet-switching table
```

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static

SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC)

Ethernet switching table : 30 entries, 30 learned

Routing instance : default-switch

Vlan	MAC	MAC	Logical	Active
name	address	flags	interface	source
v100	00:31:46:e8:f9:d6	D	vtep.32768	
192.168.2.22				
v100	7c:e2:ca:e2:75:7c	D	vtep.32771	
192.168.4.44				
v100	7c:e2:ca:e4:05:9a	D	vtep.32770	
192.168.3.33				
v101	00:31:46:e8:f9:d6	D	vtep.32768	

192.168.2.22			
v101	7c:e2:ca:e2:75:7c	D	vtep.32771
192.168.4.44			
v101	7c:e2:ca:e4:05:9a	D	vtep.32770
192.168.3.33			
v102	00:31:46:e8:f9:d6	D	vtep.32768
192.168.2.22			
v102	7c:e2:ca:e2:75:7c	D	vtep.32771
192.168.4.44			
v102	7c:e2:ca:e4:05:9a	D	vtep.32770
192.168.3.33			
v103	00:31:46:e8:f9:d6	D	vtep.32768
192.168.2.22			
v103	7c:e2:ca:e2:75:7c	D	vtep.32771
192.168.4.44			
v103	7c:e2:ca:e4:05:9a	D	vtep.32770
192.168.3.33			
v3001	00:31:46:e8:f9:d6	D	vtep.32768
192.168.2.22			
v3001	28:c0:da:6a:9f:c2	DL	ae11.0
v3001	7c:e2:ca:e2:75:7c	D	vtep.32771
192.168.4.44			
v3001	7c:e2:ca:e4:05:9a	D	vtep.32770
192.168.3.33			
v3002	00:31:46:e8:f9:d6	D	vtep.32768
192.168.2.22			
v3002	7c:e2:ca:e2:75:7c	D	vtep.32771
192.168.4.44			
v3002	7c:e2:ca:e4:05:9a	D	vtep.32770
192.168.3.33			
v3003	00:31:46:e8:f9:d6	D	vtep.32768
192.168.2.22			
v3003	28:c0:da:6a:9f:c2	DL	ae11.0
v3003	7c:e2:ca:e2:75:7c	D	vtep.32771
192.168.4.44			
v3003	7c:e2:ca:e4:05:9a	D	vtep.32770
192.168.3.33			
v3004	00:31:46:e8:f9:d6	D	vtep.32768
192.168.2.22			
v3004	7c:e2:ca:e2:75:7c	D	vtep.32771
192.168.4.44			
v3004	7c:e2:ca:e4:05:9a	D	vtep.32770
192.168.3.33			
v3005	00:31:46:e8:f9:d6	D	vtep.32768
192.168.2.22			
v3005	28:c0:da:6a:9f:c2	DL	ae11.0
v3005	7c:e2:ca:e2:75:7c	D	vtep.32771
192.168.4.44			
v3005	7c:e2:ca:e4:05:9a	D	vtep.32770
192.168.3.33			

show ethernet-switching table brief (QFX Series, QFabric, NFX Series and EX460)

```
user@switch> show ethernet-switching table brief
```

```
Ethernet-switching table: 57 entries, 17 learned
```

VLAN	MAC address	Type	Age	Interfaces
F2	*	Flood		- All-members
F2	00:00:05:00:00:03	Learn	0	xe-0/0/44.0
F2	00:19:e2:50:7d:e0	Static		- Router

```

Linux      *      Flood      - All-members
Linux      00:19:e2:50:7d:e0 Static - Router
Linux      00:30:48:90:54:89 Learn 0 xe-0/0/47.0
T1         *      Flood      - All-members
T1         00:00:05:00:00:01 Learn 0 xe-0/0/46.0
T1         00:00:5e:00:01:00 Static - Router
T1         00:19:e2:50:63:e0 Learn 0 xe-0/0/46.0
T1         00:19:e2:50:7d:e0 Static - Router
T10        *      Flood      - All-members
T10        00:00:5e:00:01:09 Static - Router
T10        00:19:e2:50:63:e0 Learn 0 xe-0/0/46.0
T10        00:19:e2:50:7d:e0 Static - Router
T111       *      Flood      - All-members
T111       00:19:e2:50:63:e0 Learn 0 xe-0/0/15.0
T111       00:19:e2:50:7d:e0 Static - Router
T111       00:19:e2:50:ac:00 Learn 0 xe-0/0/15.0
T2         *      Flood      - All-members
T2         00:00:5e:00:01:01 Static - Router
T2         00:19:e2:50:63:e0 Learn 0 xe-0/0/46.0
T2         00:19:e2:50:7d:e0 Static - Router
T3         *      Flood      - All-members
T3         00:00:5e:00:01:02 Static - Router
T3         00:19:e2:50:63:e0 Learn 0 xe-0/0/46.0
T3         00:19:e2:50:7d:e0 Static - Router
T4         *      Flood      - All-members
T4         00:00:5e:00:01:03 Static - Router
T4         00:19:e2:50:63:e0 Learn 0 xe-0/0/46.0
[output truncated]

```

show ethernet-switching table detail (QFX Series, QFabric, NFX Series and EX460)

```

user@switch> show ethernet-switching table detail

Ethernet-switching table: 57 entries, 17 learned
F2, *
  Interface(s): xe-0/0/44.0
  Type: Flood
  Nexthop index: 0

F2, 00:00:05:00:00:03
  Interface(s): xe-0/0/44.0
  Type: Learn, Age: 0, Learned: 2:03:09
  Nexthop index: 0

F2, 00:19:e2:50:7d:e0
  Interface(s): Router
  Type: Static
  Nexthop index: 0

Linux, *
  Interface(s): xe-0/0/47.0
  Type: Flood
  Nexthop index: 0

Linux, 00:19:e2:50:7d:e0
  Interface(s): Router
  Type: Static
  Nexthop index: 0

Linux, 00:30:48:90:54:89

```

```

Interface(s): xe-0/0/47.0
Type: Learn, Age: 0, Learned: 2:03:08
Nexthop index: 0

T1, *
Interface(s): xe-0/0/46.0
Type: Flood
Nexthop index: 0

T1, 00:00:05:00:00:01
Interface(s): xe-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
Nexthop index: 0

T1, 00:00:5e:00:01:00
Interface(s): Router
Type: Static
Nexthop index: 0

T1, 00:19:e2:50:63:e0
Interface(s): xe-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
Nexthop index: 0

T1, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Nexthop index: 0

T10, *
Interface(s): xe-0/0/46.0
Type: Flood
Nexthop index: 0

T10, 00:00:5e:00:01:09
Interface(s): Router
Type: Static
Nexthop index: 0

T10, 00:19:e2:50:63:e0
Interface(s): xe-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:08
Nexthop index: 0

T10, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Nexthop index: 0

T111, *
Interface(s): xe-0/0/15.0
Type: Flood
Nexthop index: 0
[output truncated]

```

show ethernet-switching table extensive (QFX Series, QFabric, NFX Series and EX460)

```
user@switch> show ethernet-switching table extensive
```

Ethernet-switching table: 57 entries, 17 learned

F2, *

Interface(s): xe-0/0/44.0

Type: Flood

Nexthop index: 0

F2, 00:00:05:00:00:03

Interface(s): xe-0/0/44.0

Type: Learn, Age: 0, Learned: 2:03:09

Nexthop index: 0

F2, 00:19:e2:50:7d:e0

Interface(s): Router

Type: Static

Nexthop index: 0

Linux, *

Interface(s): xe-0/0/47.0

Type: Flood

Nexthop index: 0

Linux, 00:19:e2:50:7d:e0

Interface(s): Router

Type: Static

Nexthop index: 0

Linux, 00:30:48:90:54:89

Interface(s): xe-0/0/47.0

Type: Learn, Age: 0, Learned: 2:03:08

Nexthop index: 0

T1, *

Interface(s): xe-0/0/46.0

Type: Flood

Nexthop index: 0

T1, 00:00:05:00:00:01

Interface(s): xe-0/0/46.0

Type: Learn, Age: 0, Learned: 2:03:07

Nexthop index: 0

T1, 00:00:5e:00:01:00

Interface(s): Router

Type: Static

Nexthop index: 0

T1, 00:19:e2:50:63:e0

Interface(s): xe-0/0/46.0

Type: Learn, Age: 0, Learned: 2:03:07

Nexthop index: 0

T1, 00:19:e2:50:7d:e0

Interface(s): Router

Type: Static

Nexthop index: 0

T10, *

Interface(s): xe-0/0/46.0

Type: Flood

Nexthop index: 0

```

T10, 00:00:5e:00:01:09
  Interface(s): Router
  Type: Static
  Nexthop index: 0

T10, 00:19:e2:50:63:e0
  Interface(s): xe-0/0/46.0
  Type: Learn, Age: 0, Learned: 2:03:08
  Nexthop index: 0

T10, 00:19:e2:50:7d:e0
  Interface(s): Router
  Type: Static
  Nexthop index: 0

T111, *
  Interface(s): xe-0/0/15.0
  Type: Flood
  Nexthop index: 0
[output truncated]

```

show ethernet-switching table interface (QFX Series, QFabric, NFX Series and EX460)

```
user@switch> show ethernet-switching table interface xe-0/0/1
```

```

Ethernet-switching table: 1 unicast entries
VLAN      MAC address      Type      Age Interfaces
V1         *                Flood     - All-members
V1         00:00:05:00:00:05 Learn      0 xe-0/0/1.0

```

show ethernet-switching table (EX Series switches)

```
user@switch> show ethernet-switching table
```

```

Ethernet-switching table: 57 entries, 15 learned, 2 persistent
VLAN      MAC address      Type      Age Interfaces
F2         *                Flood     - All-members
F2         00:00:05:00:00:03 Learn      0 ge-0/0/44.0
F2         00:19:e2:50:7d:e0 Static    - Router
Linux      *                Flood     - All-members
Linux      00:19:e2:50:7d:e0 Static    - Router
Linux      00:30:48:90:54:89 Learn      0 ge-0/0/47.0
T1         *                Flood     - All-members
T1         00:00:05:00:00:01 Persistent 0 ge-0/0/46.0
T1         00:00:5e:00:01:00 Static    - Router
T1         00:19:e2:50:63:e0 Persistent 0 ge-0/0/46.0
T1         00:19:e2:50:7d:e0 Static    - Router
T10        *                Flood     - All-members
T10        00:00:5e:00:01:09 Static    - Router
T10        00:19:e2:50:63:e0 Learn      0 ge-0/0/46.0
T10        00:19:e2:50:7d:e0 Static    - Router
T111       *                Flood     - All-members
T111       00:19:e2:50:63:e0 Learn      0 ge-0/0/15.0
T111       00:19:e2:50:7d:e0 Static    - Router
T111       00:19:e2:50:ac:00 Learn      0 ge-0/0/15.0
T2         *                Flood     - All-members
T2         00:00:5e:00:01:01 Static    - Router
T2         00:19:e2:50:63:e0 Learn      0 ge-0/0/46.0

```

```

T2          00:19:e2:50:7d:e0 Static      - Router
T3          *                      Flood    - All-members
T3          00:00:5e:00:01:02 Static      - Router
T3          00:19:e2:50:63:e0 Learn       0 ge-0/0/46.0
T3          00:19:e2:50:7d:e0 Static      - Router
T4          *                      Flood    - All-members
T4          00:00:5e:00:01:03 Static      - Router
T4          00:19:e2:50:63:e0 Learn       0 ge-0/0/46.0
[output truncated]

```

show ethernet-switching table brief (EX Series switches)

```

user@switch> show ethernet-switching table brief

Ethernet-switching table: 57 entries, 15 learned, 2 persistent entries
VLAN      MAC address      Type      Age Interfaces
F2        *                Flood     - All-members
F2        00:00:05:00:00:03 Learn     0 ge-0/0/44.0
F2        00:19:e2:50:7d:e0 Static    - Router
Linux     *                Flood     - All-members
Linux     00:19:e2:50:7d:e0 Static    - Router
Linux     00:30:48:90:54:89 Learn     0 ge-0/0/47.0
T1        *                Flood     - All-members
T1        00:00:05:00:00:01 Persistent 0 ge-0/0/46.0
T1        00:00:5e:00:01:00 Static    - Router
T1        00:19:e2:50:63:e0 Persistent 0 ge-0/0/46.0
T1        00:19:e2:50:7d:e0 Static    - Router
T10       *                Flood     - All-members
T10       00:00:5e:00:01:09 Static    - Router
T10       00:19:e2:50:63:e0 Learn     0 ge-0/0/46.0
T10       00:19:e2:50:7d:e0 Static    - Router
T111     *                Flood     - All-members
T111     00:19:e2:50:63:e0 Learn     0 ge-0/0/15.0
T111     00:19:e2:50:7d:e0 Static    - Router
T111     00:19:e2:50:ac:00 Learn     0 ge-0/0/15.0
T2        *                Flood     - All-members
T2        00:00:5e:00:01:01 Static    - Router
T2        00:19:e2:50:63:e0 Learn     0 ge-0/0/46.0
T2        00:19:e2:50:7d:e0 Static    - Router
T3        *                Flood     - All-members
T3        00:00:5e:00:01:02 Static    - Router
T3        00:19:e2:50:63:e0 Learn     0 ge-0/0/46.0
T3        00:19:e2:50:7d:e0 Static    - Router
T4        *                Flood     - All-members
T4        00:00:5e:00:01:03 Static    - Router
T4        00:19:e2:50:63:e0 Learn     0 ge-0/0/46.0
[output truncated]

```

show ethernet-switching table detail (EX Series switches)

```

user@switch> show ethernet-switching table detail

Ethernet-switching table: 5 entries, 2 learned entries
VLAN: default, Tag: 0, MAC: *, Interface: All-members
Interfaces:
  ge-0/0/11.0, ge-0/0/20.0, ge-0/0/30.0, ge-0/0/36.0, ge-0/0/3.0
Type: Flood
Nexthop index: 1307

```



```

VLAN: default, Tag: 0, MAC: 00:1f:12:30:b8:83, Interface: ge-0/0/3.0
  Type: Learn, Age: 0, Learned: 20:09:26
  Nexthop index: 1315

VLAN: v1, Tag: 101, MAC: *, Interface: All-members
  Interfaces:
    ge-0/0/31.0
  Type: Flood
  Nexthop index: 1313

VLAN: v1, Tag: 101, MAC: 00:1f:12:30:b8:89, Interface: ge-0/0/31.0
  Type: Learn, Age: 0, Learned: 20:09:25
  Nexthop index: 1312

VLAN: v2, Tag: 102, MAC: *, Interface: All-members
  Interfaces:
    ae0.0
  Type: Flood
  Nexthop index: 1317

```

show ethernet-switching table extensive (EX Series switches)

```
user@switch> show ethernet-switching table extensive
```

```
Ethernet-switching table: 3 entries, 1 learned, 5 persistent entries
```

```

VLAN: v1, Tag: 10, MAC: *, Interface: All-members
  Interfaces:
    ge-0/0/14.0, ge-0/0/1.0, ge-0/0/2.0, ge-0/0/3.0, ge-0/0/4.0,
    ge-0/0/5.0, ge-0/0/6.0, ge-0/0/7.0, ge-0/0/8.0, ge-0/0/10.0,
    ge-0/0/0.0
  Type: Flood
  Nexthop index: 567

VLAN: v1, Tag: 10, MAC: 00:21:59:c6:93:22, Interface: Router
  Type: Static
  Nexthop index: 0

VLAN: v1, Tag: 10, MAC: 00:21:59:c9:9a:4e, Interface: ge-0/0/14.0
  Type: Learn, Age: 0, Learned: 18:40:50
  Nexthop index: 564

```

show ethernet-switching table persistent-mac (EX Series switches)

```
user@switch> show ethernet-switching table persistent-mac
```

VLAN	MAC address	Type	Interface
default	00:10:94:00:00:02	installed	ge-0/0/42.0
default	00:10:94:00:00:03	installed	ge-0/0/42.0
default	00:10:94:00:00:04	installed	ge-0/0/42.0
default	00:10:94:00:00:05	installed	ge-0/0/42.0
default	00:10:94:00:00:06	installed	ge-0/0/42.0
default	00:10:94:00:05:02	uninstalled	ge-0/0/16.0
default	00:10:94:00:06:03	uninstalled	ge-0/0/16.0
default	00:10:94:00:07:04	uninstalled	ge-0/0/16.0

show ethernet-switching table persistent-mac interface ge-0/0/16.0 (EX Series switches)

VLAN	MAC address	Type	Interface
default	00:10:94:00:05:02	uninstalled	ge-0/0/16.0
default	00:10:94:00:06:03	uninstalled	ge-0/0/16.0
default	00:10:94:00:07:04	uninstalled	ge-0/0/16.0

show ethernet-switching table (EX Series, MX Series and QFX Series)

```
user@host> show ethernet-switching table
```

```
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
```

```
Routing instance : default-switch
```

Vlan	MAC	MAC	Age	Logical
name	address	flags		interface
VLAN101	88:e0:f3:bb:07:f0	D	-	ae20.0

```
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
```

```
Routing instance : default-switch
```

Vlan	MAC	MAC	Age	Logical
name	address	flags		interface
VLAN102	88:e0:f3:bb:07:f0	D	-	ae20.0

```
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
```

```
Routing instance : default-switch
```

Vlan	MAC	MAC	Age	Logical
name	address	flags		interface
VLAN103	88:e0:f3:bb:07:f0	D	-	ae20.0

```
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
```

```
Routing instance : default-switch
```

Vlan	MAC	MAC	Age	Logical
name	address	flags		interface
VLAN104	88:e0:f3:bb:07:f0	D	-	ae20.0

```
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
```

```
Routing instance : default-switch
```

Vlan	MAC	MAC	Age	Logical
name	address	flags		interface
VLAN1101	00:1f:12:32:f5:c1	D	-	ae0.0

```
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
```

```

Routing instance : default-switch
  Vlan      MAC      MAC      Age      Logical
  name      address   flags                interface
  VLAN1102  00:1f:12:32:f5:c1 D        -        ae0.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
  Vlan      MAC      MAC      Age      Logical
  name      address   flags                interface
  VLAN1103  00:1f:12:32:f5:c1 D        -        ae0.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
  Vlan      MAC      MAC      Age      Logical
  name      address   flags                interface
  VLAN1104  00:1f:12:32:f5:c1 D        -        ae0.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
  Vlan      MAC      MAC      Age      Logical
  name      address   flags                interface
  VLAN1105  00:1f:12:32:f5:c1 D        -        ae0.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
  Vlan      MAC      MAC      Age      Logical
  name      address   flags                interface
  VLAN1106  00:1f:12:32:f5:c1 D        -        ae0.0
[...output truncated...]

```

show ethernet-switching table brief

```

user@host> show ethernet-switching table brief

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
  Vlan      MAC      MAC      Age      Logical
  name      address   flags                interface
  VLAN101   88:e0:f3:bb:07:f0 D        -        ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
  Vlan      MAC      MAC      Age      Logical

```

```

name          address          flags          interface
VLAN102       88:e0:f3:bb:07:f0    D              -      ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan          MAC          MAC          Age          Logical
name          address        flags         interface
VLAN103       88:e0:f3:bb:07:f0    D              -      ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan          MAC          MAC          Age          Logical
name          address        flags         interface
VLAN104       88:e0:f3:bb:07:f0    D              -      ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan          MAC          MAC          Age          Logical
name          address        flags         interface
VLAN1101      00:1f:12:32:f5:c1    D              -      ae0.0
[...output truncated...]

```

show ethernet-switching table count

```

user@host> show ethernet-switching table count

0 MAC address learned in routing instance default-switch VLAN VLAN1000
ae26.0:1000

1 MAC address learned in routing instance default-switch VLAN VLAN101
ae20.0:101

MAC address count per learn VLAN within routing instance:
  Learn VLAN ID      MAC count      Static MAC count
      101              1                0

1 MAC address learned in routing instance default-switch VLAN VLAN102
ae20.0:102

MAC address count per learn VLAN within routing instance:
  Learn VLAN ID      MAC count      Static MAC count
      102              1                0

1 MAC address learned in routing instance default-switch VLAN VLAN103
ae20.0:103

MAC address count per learn VLAN within routing instance:
  Learn VLAN ID      MAC count      Static MAC count
      103              1                0

1 MAC address learned in routing instance default-switch VLAN VLAN104

```

```

ae20.0:104

  MAC address count per learn VLAN within routing instance:
    Learn VLAN ID      MAC count      Static MAC count
          104             1             0

0 MAC address learned in routing instance default-switch VLAN VLAN105
ae20.0:105

0 MAC address learned in routing instance default-switch VLAN VLAN106
ae20.0:106

0 MAC address learned in routing instance default-switch VLAN VLAN107
ae20.0:107

0 MAC address learned in routing instance default-switch VLAN VLAN108
ae20.0:108

0 MAC address learned in routing instance default-switch VLAN VLAN109
ae20.0:109

0 MAC address learned in routing instance default-switch VLAN VLAN110
ae20.0:110

1 MAC address learned in routing instance default-switch VLAN VLAN1101
ae0.0:1101

  MAC address count per learn VLAN within routing instance:
    Learn VLAN ID      MAC count      Static MAC count
          1101             1             0

1 MAC address learned in routing instance default-switch VLAN VLAN1102
ae0.0:1102

  MAC address count per learn VLAN within routing instance:
    Learn VLAN ID      MAC count      Static MAC count
          1102             1             0
[...output truncated...]

```

show ethernet-switching table extensive

```
user@host> show ethernet-switching table extensive
```

```

MAC address: 88:e0:f3:bb:07:f0
  Routing instance: default-switch
  VLAN ID: 101
    Learning interface: ae20.0
    Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
    Epoch: 0                      Sequence number: 2
    Learning mask: 0x00000008

MAC address: 88:e0:f3:bb:07:f0
  Routing instance: default-switch
  VLAN ID: 102
    Learning interface: ae20.0
    Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
    Epoch: 0                      Sequence number: 2
    Learning mask: 0x00000008

```

```

MAC address: 88:e0:f3:bb:07:f0
  Routing instance: default-switch
VLAN ID: 103
  Learning interface: ae20.0
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 2
  Learning mask: 0x00000008

MAC address: 88:e0:f3:bb:07:f0
  Routing instance: default-switch
VLAN ID: 104
  Learning interface: ae20.0
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 2
  Learning mask: 0x00000008

MAC address: 00:1f:12:32:f5:c1
  Routing instance: default-switch
VLAN ID: 1101
  Learning interface: ae0.0
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 2
  Learning mask: 0x00000008

MAC address: 00:1f:12:32:f5:c1
  Routing instance: default-switch
VLAN ID: 1102
  Learning interface: ae0.0
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 2
  Learning mask: 0x00000008

MAC address: 00:1f:12:32:f5:c1
  Routing instance: default-switch
VLAN ID: 1103
  Learning interface: ae0.0
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 2
  Learning mask: 0x00000008

MAC address: 00:1f:12:32:f5:c1
  Routing instance: default-switch
VLAN ID: 1104
  Learning interface: ae0.0
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 2
  Learning mask: 0x00000008

```

Sample Output

show ethernet-switching table detail (SRX Series)

```

user@host> show ethernet-switching table detail

Ethernet-switching table: 57 entries, 17 learned
F2, *
Interface(s): ge-0/0/44.0
Type: Flood
F2, 00:00:5E:00:53:AC
Interface(s): ge-0/0/44.0

```

```

Type: Learn, Age: 0, Learned: 2:03:09
F2, 00:00:5E:00:53:AA
Interface(s): Router
Type: Static
Linux, *
Interface(s): ge-0/0/47.0
Type: Flood
Linux, 00:00:5E:00:53:AB
Interface(s): Router
Type: Static
Linux, 00:00:5E:00:53:AC
Interface(s): ge-0/0/47.0
Type: Learn, Age: 0, Learned: 2:03:08
T1, *
Interface(s): ge-0/0/46.0
Type: Flood
T1, 00:00:5E:00:53:AD
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:00:5E:00:53:AE
Interface(s): Router
Type: Static
T1, 00:00:5E:00:53:AF
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:00:5E:00:53:AG
Interface(s): Router
Type: Static
T10, *
Interface(s): ge-0/0/46.0
Type: Flood
T10, 00:00:5E:00:53:AH
Interface(s): Router
Type: Static
T10, 00:00:5E:00:53:AI
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:08
T10, 00:00:5E:00:53:AJ
Interface(s): Router
Type: Static
T111, *
Interface(s): ge-0/0/15.0
Type: Flood
[output truncated]

```

Sample Output

show ethernet-switching table extensive (SRX Series)

```

user@host> show ethernet-switching table extensive

Ethernet-switching table: 57 entries, 17 learned
F2, *
Interface(s): ge-0/0/44.0
Type: Flood
F2, 00:00:5E:00:53:AC
Interface(s): ge-0/0/44.0
Type: Learn, Age: 0, Learned: 2:03:09
F2, 00:00:5E:00:53:AA
Interface(s): Router

```

```

Type: Static
Linux, *
Interface(s): ge-0/0/47.0
Type: Flood
Linux, 00:00:5E:00:53:AB
Interface(s): Router
Type: Static
Linux, 00:00:5E:00:53:AC
Interface(s): ge-0/0/47.0
Type: Learn, Age: 0, Learned: 2:03:08
T1, *
Interface(s): ge-0/0/46.0
Type: Flood
T1, 00:00:5E:00:53:AD
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:00:5E:00:53:AE
Interface(s): Router
Type: Static
T1, 00:00:5E:00:53:AF
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
T1, 00:00:5E:00:53:AG
Interface(s): Router
Type: Static
T10, *
Interface(s): ge-0/0/46.0
Type: Flood
T10, 00:00:5E:00:53:AH
Interface(s): Router
Type: Static
T10, 00:00:5E:00:53:AI
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:08
T10, 00:00:5E:00:53:AJ
Interface(s): Router
Type: Static
T111, *
Interface(s): ge-0/0/15.0
Type: Flood
[output truncated]

```

Sample Output

show ethernet-switching table interface ge-0/0/1 (SRX Series)

```

user@host> show ethernet-switching table interface ge-0/0/1

Ethernet-switching table: 1 unicast entries
VLAN      MAC address      Type    Age Interfaces
V1        *                Flood   - All-members
V1        00:00:5E:00:53:AF Learn    0 ge-0/0/1.0

```


show ike security-associations

Syntax `show ike security-associations`
`<brief | detail>`
`<peer-address>`

Release Information Command introduced before Junos OS Release 7.4.

Description (Encryption interface on M Series and T Series routers only) Display information about Internet Key Exchange (IKE) security associations.

Options **none**—Display standard information about all IKE security associations.

brief | detail—(Optional) Display the specified level of output.

peer-address—(Optional) Display IKE security associations for the specified peer address.

Required Privilege Level view

Related Documentation

- *clear ike security-associations*

List of Sample Output [show ike security-associations on page 1224](#)
[show ike security-associations detail on page 1224](#)

Output Fields [Table 65 on page 1221](#) lists the output fields for the **show ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 65: show ike security-associations Output Fields

Field Name	Field Description	Level of Output
IKE peer	Remote end of the IKE negotiation.	detail
Role	Part played in the IKE session. The router triggering the IKE negotiation is the initiator, and the router accepting the first IKE exchange packets is the responder.	detail
Remote Address	Responder's address.	none specified
State	State of the IKE security association: <ul style="list-style-type: none"> • Matured—The IKE security association is established. • Not matured—The IKE security association is in the process of negotiation. 	none specified
Initiator cookie	When the IKE negotiation is triggered, a random number is sent to the remote node.	All levels

Table 65: show ike security-associations Output Fields (continued)

Field Name	Field Description	Level of Output
Responder cookie	<p>The remote node generates its own random number and sends it back to the initiator as a verification that the packets were received.</p> <p>Of the numerous security services available, protection against denial of service (DoS) is one of the most difficult to address. A “cookie” or anticlogging token (ACT) is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity. An exchange prior to CPU-intensive public key operations can thwart some DoS attempts (such as simple flooding with invalid IP source addresses).</p>	All levels
Exchange type	<p>Specifies the number of messages in an IKE exchange, and the payload types that are contained in each message. Each exchange type provides a particular set of security services, such as anonymity of the participants, perfect forward secrecy of the keying material, and authentication of the participants. Junos OS supports two types of exchanges:</p> <ul style="list-style-type: none"> • Main—The exchange is done with six messages. Main encrypts the payload, protecting the identity of the neighbor. • Aggressive—The exchange is done with three messages. Aggressive does not encrypt the payload, leaving the identity of the neighbor unprotected. 	All Levels
Authentication method	Type of authentication determines which payloads are exchanged and when they are exchanged. The Junos OS supports only pre-shared keys .	detail
Local	Prefix and port number of the local end.	detail
Remote	Prefix and port number of the remote end.	detail
Lifetime	Number of seconds remaining until the IKE security association expires.	detail
Algorithms	<p>Header for the IKE algorithms output.</p> <ul style="list-style-type: none"> • Authentication—Type of authentication algorithm used: md5 or sha1. • Encryption—Type of encryption algorithm used: des-cbc, 3des-cbc, or None. • Pseudo random function—Function that generates highly unpredictable random numbers: hmac-md5 or hmac-sha1. 	detail
Traffic statistics	<p>Number of bytes and packets received and transmitted on the IKE security association.</p> <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the IKE security association. • Input packets, Output packets—Number of packets received and transmitted on the IKE security association. 	detail

Table 65: show ike security-associations Output Fields (continued)

Field Name	Field Description	Level of Output
Flags	Notification to the key management process of the status of the IKE negotiation: <ul style="list-style-type: none"> • caller notification sent—Caller program notified about the completion of the IKE negotiation. • waiting for done—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. • waiting for remove—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. • waiting for policy manager—Negotiation is waiting for a response from the policy manager. 	detail
IPsec security associates	Number of IPsec security associations created and deleted with this IKE security association.	detail
Phase 2 negotiations in progress	Number of phase 2 IKE negotiations in progress and status information: <ul style="list-style-type: none"> • Negotiation type—Type of phase 2 negotiation. The Junos OS currently supports quick mode. • Message ID—Unique identifier for a phase 2 negotiation. • Local identity—Identity of the local phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[O..id-data-len] = iddata-presentation)</i> • Remote identity—Identity of the remote phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[O..id-data-len] = iddata-presentation)</i> • Flags—Notification to the key management process of the status of the IKE negotiation: <ul style="list-style-type: none"> • caller notification sent—Caller program notified about the completion of the IKE negotiation. • waiting for done—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. • waiting for remove—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. • waiting for policy manager—Negotiation is waiting for a response from the policy manager. 	detail

Sample Output

show ike security-associations

```
user@host> show ike security-associations
```

Remote Address	State	Initiator cookie	Responder cookie	Exchange type
192.0.2.4	Matured	93870456fa000011	723a20713700003e	Main

show ike security-associations detail

```
user@host> show ike security-associations detail
```

```
IKE peer 192.0.2.4
  Role: Initiator, State: Matured
  Initiator cookie: cf22bd81a7000001, Responder cookie: fe83795c2800002e
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 192.0.2.5:500, Remote: 192.0.2.4:500
  Lifetime: Expires in 187 seconds
  Algorithms:
    Authentication      : md5
    Encryption          : 3des-cbc
    Pseudo random function: hmac-md5
  Traffic statistics:
    Input bytes  :          1000
    Output bytes :          1280
    Input packets:           5
    Output packets:          9
  Flags: Caller notification sent
  IPsec security associations: 2 created, 0 deleted
  Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 3582889153
  Local: 192.0.2.5:500, Remote: 192.0.2.4:500
  Local identity: ipv4_subnet(tcp:80,[0..7]=10.1.1.0/24)
  Remote identity: ipv4_subnet(tcp:100,[0..7]=10.1.2.0/24)
  Flags: Caller notification sent, Waiting for done
```

show ipsec certificates

Syntax `show ipsec certificates`
`<brief | detail>`
`<crl crl-name | serial-number>`

Release Information Command introduced before Junos OS Release 7.4.

Description (Encryption interface on M Series and T Series routers only) Display information about the IPsec certificate database.

Options **none**—Display standard information about all of the entries in the IPsec certificate database.

brief | detail—(Optional) Display the specified level of output.

crl *crl-name* | *serial-number*—(Optional) Display information about the entries on the certificate revocation list (CRL) or for the specified serial number. A CRL is a timestamped list identifying revoked certificates. The CRL is signed by a certificate authority (CA) or CRL issuer and made freely available in a public repository. Each revoked certificate is identified in a CRL by its certificate serial number.

Required Privilege Level view

Related Documentation

- *clear ipsec security-associations*

List of Sample Output [show ipsec certificates detail on page 1226](#)

Output Fields [Table 66 on page 1225](#) lists the output fields for the **show ipsec certificates** command. Output fields are listed in the approximate order in which they appear.

Table 66: show ipsec certificates Output Fields

Field Name	Field Description	Level of Output
Database	Display information about the IPsec certificate database. <ul style="list-style-type: none"> • Total entries—Number of database entries, including entries that are not trusted or that are in the process of being deleted. • Active entries—Number of database entries, excluding entries that are marked as deleted. • Locked entries—Number of statically configured database entries that cannot expire, such as CA certificates that are root or trusted. 	All levels
Subject	Distinguished name for the certificate for C, O, CN , as described in RFC 3280, <i>Internet x.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile</i> .	All levels

Table 66: show ipsec certificates Output Fields (continued)

Field Name	Field Description	Level of Output
ID	Identification number of the database entry. ID is generated by the internal certificate database.	All levels
References	Reference number the certificate manager has for the particular entry.	detail
Serial	Unique serial number assigned to each certificate by the CA.	All levels
Flags	State of the certificate. <ul style="list-style-type: none"> • Trusted—Passed validity checks. • Not trusted—Failed validity checks. • Root—Entry is locked and may have been learned through IKE or a locally configured CA certificate. • Non-root—Entry is not locked. • Crl-issuer—Entity issues CRLs. • Non-crl-issuer—Entity does not issue CRLs. 	detail
Validity period starts	Start time that the certificate is valid, in the format <i>yyyy mon dd, hh:mm:ss GMT</i> .	detail
Validity period ends	End time that the certificate is valid, in the format <i>yyyy mon dd, hh:mm:ss GMT</i> .	detail
Alternative name information	Auxiliary identity for the certificate: <i>dns-name</i> , <i>email-address</i> , <i>ip-address</i> , or <i>uri</i> (uniform resource identifier).	detail
Issuer	Information about the entity that has signed and issued the CRL as described in RFC 2459, <i>Internet X.509 Public Key Infrastructure Certificate and CRL Profile</i> .	detail

Sample Output

show ipsec certificates detail

```

user@host> show ipsec certificates detail

Database: Total entries: 3 Active entries: 4 Locked entries: 1
Subject: C=us, O=x
  ID: 5, References: 0, Serial: 22314868
  Flags: Trusted Non-root Crl-issuer
  Validity period starts: 2003 Mar 1st, 01:20:42 GMT
  Validity period ends: 2003 Mar 31st, 01:50:42 GMT
  Alternative name information:
    IP address: 10.20.210.1
  Issuer: C=FI, O=Company-ABC, CN=Company ABC class 2

Subject: C=us, O=x
  ID: 4, References: 0, Serial: 22315496
  Flags: Trusted Non-root Crl-issuer
  Validity period starts: 2003 Mar 1st, 01:21:45 GMT
  Validity period ends: 2003 Mar 31st, 01:51:45 GMT
  Alternative name information:
    IP address: 10.20.210.20

```

```
Issuer: C=FI, O=Company-ABC, CN=Company ABC class 2
Subject: C=FI, O=SSH Company-ABC, CN=Company ABC class 2
ID: 1, References: 1, Serial: 1538512
Flags: Trusted Root Non-crl-issuer
Validity period starts: 2001 Aug 1st, 07:08:32 GMT
Validity period ends: 2004 Aug 1st, 07:08:32 GMT
Alternative name information:
  Email address: certifier-support@ssh.com
Issuer: C=FI, O=Company-ABC, CN=Company ABC class 2
```

show ipsec security-associations

Syntax `show ipsec security-associations
<brief | detail>
<sa-name>`

Release Information Command introduced before Junos OS Release 7.4.

Description Display information about the IPsec security associations applied to the local or transit traffic stream.

Options **none**—Display standard information about all IPsec security associations.

brief | detail—(Optional) Display the specified level of output.

sa-name—(Optional) Display the specified IPsec security association.

Required Privilege Level view

List of Sample Output [show ipsec security-associations sa-name on page 1230](#)
[show ipsec security-associations sa-name detail on page 1230](#)

Output Fields [Table 67 on page 1228](#) lists the output fields for the **show ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 67: show ipsec security-associations Output Fields

Field Name	Field Description	Level of Output
Security association	Name of the security association.	All levels
Interface family	Status of the interface family of the security association. If the interface family field is absent, it is a transport mode security association. The interface family can have one of three options: <ul style="list-style-type: none"> • Up—The security association is referenced in the interface family and the interface family is up. • Down—The security association is referenced in the interface family and the interface family is down. • No reference—The security association is not referenced in the interface family. 	All levels
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels
Local identity	Prefix and port number of the local end	All levels
Remote identity	Prefix and port number of the remote end.	All levels

Table 67: show ipsec security-associations Output Fields (continued)

Field Name	Field Description	Level of Output
Direction	Direction of the security association: inbound or outbound .	All levels
SPI	Value of the security parameter index.	All levels
AUX-SPI	Value of the auxiliary security parameter index. <ul style="list-style-type: none"> When the value is AH or ESP, AUX-SPI is always 0. When the value is AH+ESP, AUX-SPI is always a positive integer. 	All levels
State	Status of the security association: <ul style="list-style-type: none"> Installed—The security association is installed in the security association database. (For transport mode security associations, the value of State must always be Installed.) Not installed—The security association is not installed in the security association database. 	detail
Mode	Mode of the security association: <ul style="list-style-type: none"> transport—Protects single host-to-host protections. tunnel—Protects connections between security gateways. 	All levels
Type	Type of security association: <ul style="list-style-type: none"> manual—Security parameters require no negotiation. They are static, and are configured by the user. dynamic—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode. 	All levels
Protocol	Protocol supported: <ul style="list-style-type: none"> transport mode—Supports Encapsulation Security Protocol (ESP) or Authentication Header (AH). tunnel mode—Supports ESP or AH+ESP. 	All levels
Authentication	Type of authentication used: hmac-md5-96 , hmac-sha1-96 , or None .	detail
Encryption	Type of encryption used: des-cbc , 3des-csc , or None .	detail
Soft lifetime Hard lifetime	(dynamic output only) Each lifetime of a security association has two display options, hard and soft, one of which must be present for a dynamic security association. The hard lifetime specifies the lifetime of the SA. The soft lifetime , which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires. <ul style="list-style-type: none"> Expires in seconds seconds—Number of seconds left until the security association expires. Expires in kilobytes kilobytes—Number of kilobytes left until the security association expires. 	detail

Table 67: show ipsec security-associations Output Fields (continued)

Field Name	Field Description	Level of Output
Anti-replay service	State of the service that prevents packets from being replayed: Enabled or Disabled .	detail
Replay window size	Configured size, in packets, of the antireplay service window: 32 or 64 . The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. If the replay window size is 0 , the antireplay service is disabled.	detail

Sample Output

show ipsec security-associations sa-name

```
user@host> show ipsec security-associations sa-cosmic brief

Security association: sa-cosmic, Interface family: Up
Local gateway: 192.0.2.1, Remote gateway: 198.51.100.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Direction SPI      AUX-SPI      Mode      Type      Protocol
inbound  2908734119  0          tunnel    dynamic   AH
outbound 3494029335  0          tunnel    dynamic   AH
```

show ipsec security-associations sa-name detail

```
user@host> show ipsec security-associations sa-cosmic detail

Security association: sa-cosmic, Interface family: Up

Local gateway: 192.0.2.1, Remote gateway: 198.51.100.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Direction: inbound, SPI: 2908734119, AUX-SPI: 0, State: Installed
Mode: tunnel, Type: dynamic
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Soft lifetime: Expired
Hard lifetime: Expires in 120 seconds
Anti-replay service: Disabled

Direction: outbound, SPI: 3494029335, AUX-SPI: 0, State: Installed
Mode: tunnel, Type: dynamic
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Soft lifetime: Expired
Hard lifetime: Expires in 120 seconds
Anti-replay service: Disabled
```

show ip-source-guard

Syntax	<code>show ip-source-guard</code>
Release Information	Command introduced in Junos OS Release 9.2 for EX Series switches.
Description	Display IP source guard database information.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 467 • Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 476 • Verifying That IP Source Guard Is Working Correctly on page 466
List of Sample Output	show ip-source-guard on page 1232
Output Fields	Table 68 on page 1231 lists the output fields for the <code>show ip-source-guard</code> command. Output fields are listed in the approximate order in which they appear.

Table 68: show ip-source-guard Output Fields

Field Name	Field Description
VLAN	VLAN on which IP source guard is enabled.
Interface	Access interface associated with the VLAN in column 1.
Tag	VLAN ID for the VLAN in column 1. Possible values are: <ul style="list-style-type: none"> • 0, indicating the VLAN is not tagged. • 1 – 4093
IP Address	Source IP address for a device connected to the interface in column 2. A value of * (star, or asterisk) indicates that IP source guard is not enabled on this VLAN but the interface is shared with a VLAN that is enabled for IP source guard.
MAC Address	Source MAC address for a device connected to the interface in column 2. A value of * (star, or asterisk) indicates that IP source guard is not enabled on this VLAN but the interface is shared with a VLAN that is enabled for IP source guard.

Sample Output

show ip-source-guard

```
user@switch> show ip-source-guard
```

```
IP source guard information:
```

Interface	Tag	IP Address	MAC Address	VLAN
ge-0/0/12.0	0	10.10.10.7	00:30:48:92:A5:9D	vlan100
ge-0/0/13.0	0	10.10.10.9	00:30:48:8D:01:3D	vlan100
ge-0/0/13.0	100	*	*	voice

show ipv6-source-guard

Syntax	<code>show ipv6-source-guard</code>
Release Information	Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	(For non-ELS switches) Display IPv6 source guard database information.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN on page 467 • Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces on page 476 • Verifying That IP Source Guard Is Working Correctly on page 466
List of Sample Output	show ipv6-source-guard on page 1234
Output Fields	Table 68 on page 1231 lists the output fields for the <code>show ipv6-source-guard</code> command. Output fields are listed in the approximate order in which they appear.

Table 69: show ipv6-source-guard Output Fields

Field Name	Field Description
VLAN	VLAN on which IPv6 source guard is enabled.
Interface	Access interface associated with the VLAN described in row 1.
Tag	VLAN ID for the VLAN described in row 1. Possible values are: <ul style="list-style-type: none"> • 0, indicating the VLAN is not tagged. • 1 through 4093
IP Address	Source IP address for a device connected to the interface described in row 2. A * (asterisk) indicates that IPv6 source guard is not enabled on this VLAN, but the interface is shared with a VLAN that is enabled for IPv6 source guard.
MAC Address	Source MAC address for a device connected to the interface described in row 2. A * (asterisk) indicates that IPv6 source guard is not enabled on this VLAN but the interface is shared with a VLAN that is enabled for IPv6 source guard.

Sample Output

show ipv6-source-guard

```
user@switch> show ipv6-source-guard
```

```
IP source guard information:
```

Interface	Tag	IP Address	MAC Address	VLAN
ge-0/0/6.0	0	2001:db8::10:0:15	00:10:94:10:00:01	vlan1
ge-0/0/6.0	0	fe80::210:94ff:fe10:1	00:10:94:10:00:01	vlan1
ge-0/0/7.0	0	2001:db8::10:0:14	00:10:94:10:00:02	vlan1
ge-0/0/7.0	0	fe80::210:94ff:fe10:2	00:10:94:10:00:02	vlan1

show neighbor-discovery-inspection statistics

Syntax	show neighbor-discovery-inspection statistics
Release Information	Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.
Description	Display neighbor discovery inspection statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear arp inspection statistics on page 1075 • Example: Configuring Port Security (non-ELS) on page 15 • Verifying That DAI Is Working Correctly on page 453
List of Sample Output	show neighbor-discovery-inspection statistics on page 1235
Output Fields	Table 43 on page 1130 lists the output fields for the show neighbor-discovery-inspection statistics command. Output fields are listed in the approximate order in which they appear.

Table 70: show neighbor-discovery-inspection statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which neighbor discovery inspection has been applied.	All levels
Packets received	Total number of packets total that underwent neighbor discovery inspection.	All levels
ND inspection pass	Total number of packets that passed neighbor discovery inspection.	All levels
ND inspection failed	Total number of packets that failed neighbor discovery inspection.	All levels

Sample Output

show neighbor-discovery-inspection statistics

```
user@switch> show neighbor-discovery-inspection statistics
```

Interface	Packets received	ND inspection pass	ND inspection failed
ge-0/0/0	5	1	4
ge-0/0/1	0	0	0

show security host-vpn security-associations

Syntax `show security host-vpn security-associations
<connection-name>`

Release Information Command introduced in Junos OS Evolved Release 18.3R1.

Description Display the protection details about a specified security association or all security associations.

Options **connection-name**—Specify for which connection the connection information is to be displayed. If no connection-name is specified, information for all security associations is displayed.

Additional Information The Security Parameters Index (SPI) is an arbitrary value which is used (together with the destination IP address) to identify the security association of the receiving party. Each IPsec datagram has a special field for the SPI. All datagrams in the SA will use the same SPI value in this field.

Required Privilege Level view

Related Documentation

- [clear security host-vpn security-associations on page 1070](#)
- [show security host-vpn version on page 1239](#)
- [host-vpn on page 800](#)

List of Sample Output [show security host-vpn security-associations on page 1237](#)

Output Fields [Table 71 on page 1236](#) describes the output fields for the **show security host-vpn security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 71: show security host-vpn security-associations Output Fields

Field Name	Description
IKE SA	Name of the security association connection.
ID	Identifier of the security association.

Table 71: show security host-vpn security-associations Output Fields (continued)

Field Name	Description
State	State of the parent SA connection. Values include the following: <ul style="list-style-type: none"> • CREATED—IKE SA just got created, but is not yet initiating or responding. • CONNECTING—IKE SA gets initiated actively or passively. • DESTROYING—IKE SA object gets destroyed. • ESTABLISHED—IKE SA is fully established. • PASSIVE—IKE SA is managed externally and does not process messages. • REKEYING—IKE SA rekeying is in progress.
(I:R)	Initiator and responder cookie.
local	Local endpoint information and identities.
remote	Remote endpoint information and identities.
crypto	Negotiated encryption details in effect (one for each IKE SA and child SA).
established	How long ago the SA was established, and when it rekeys.
Child SA	Name of the child SA.
State	State of the child SA connection. Values include the following: <ul style="list-style-type: none"> • CREATED—Child SA is just created, but is not yet installed. • DESTROYING—Child SA object gets destroyed. • INSTALLED—Child SA is installed and in use. • REKEYING—Child SA rekeying is in progress.
mode	IPsec mode: (transport tunnel).
in spi	Inbound SPI values. Also, shows the number of bytes and packets encrypted.
out spi	Outbound SPI values. Also, shows the number of bytes and packets encrypted.
local ts	The local traffic selector (that is, what local traffic is protected).
remote ts	The remote traffic selector (that is, what remote traffic is protected).

Sample Output

show security host-vpn security-associations

```

user@host> show security host-vpn security-associations
IKE SA : leftT1, ID:1, State:ESTABLISHED, IKEv2,
(I:R):96e7757f275c3aa1:ff01ca9e7c4590b2
  local : 10.102.227.201, id:vm1@juniper.net

```

```
remote: 10.102.228.200, id:vm1@juniper.net
crypto: AES_CBC-256/HMAC_SHA2_384_192-0/PRF_HMAC_SHA2_384/ECP_384
established 57s ago, rekey in 3295s
Child SA : childLeft1, ID:1, State:INSTALLED, mode:TUNNEL
  crypto : ESP: AES_GCM_16-256-0
  in spi : c5dfd0be, 5541188 bytes, 105772 packets
  out spi : c39dbd67, 322089572 bytes, 224729 packets
  installed: 58 s ago, rekey in 3264 s, expires in 3903 s
  local ts : [10.102.227.201/32[tcp]]
  remote ts: [10.102.228.200/32[tcp/afs3-callback]]
IKE SA : leftT2, ID:2, State:ESTABLISHED, IKEv2,
(I:R):2bd786adf65eb875:0546171950dbb490
  local : 10.102.227.201, id:vm2@juniper.net
  remote: 10.102.228.200, id:vm2@juniper.net
  crypto: AES_CBC-256/HMAC_SHA2_384_192-0/PRF_HMAC_SHA2_384/ECP_384
  established 57s ago, rekey in 3475s
  Child SA : childLeft2, ID:2, State:INSTALLED, mode:TUNNEL
    crypto : ESP: AES_GCM_16-256-0
    in spi : c0a912ee, 40 bytes, 1 packets
    out spi : c52e4bf0, 60 bytes, 1 packets
    installed: 57 s ago, rekey in 3262 s, expires in 3903 s
    local ts : [10.102.227.201/32[tcp]]
    remote ts: [10.102.228.200/32[tcp/afs3-prserver]]
```

show security host-vpn version

Syntax	show security host-vpn version
Release Information	Command introduced in Junos OS Evolved Release 18.3R1.
Description	Display the version of IPsec being used in the system.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• host-vpn on page 800

Sample Output

```
user@host> show security host-vpn version
Version: host IPsec 5.3.5 charon-systemd (Linux, 4.1.15-juniper-00909-g6846316,
x86_64)
```

show security keychain

Syntax `show security keychain
<brief | detail>`

Release Information Command introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3X50 for the QFX Series.

Description Display information about authentication keychains configured for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.

Options **none**—Display information about authentication keychains.
brief | detail—(Optional) Display the specified level of output.

Required Privilege Level view

List of Sample Output [show security keychain brief on page 1242](#)
[show security keychain detail on page 1242](#)

Output Fields [Table 72 on page 1240](#) describes the output fields for the **show security keychain** command. Output fields are listed in the approximate order in which they appear.

Table 72: show security keychain Output Fields

Field Name	Field Description	Level of Output
keychain	The name of the keychain in operation.	All levels
Active-ID Send	Number of routing protocols packets sent with the active key.	All levels
Active-ID Receive	Number of routing protocols packets received with the active key.	All levels
Next-ID Send	Number of routing protocols packets sent with the next key.	All levels
Next-ID Receive	Number of routing protocols packets received with the next key.	All levels
Transition	Amount of time until the current key will be replaced with the next key in the keychain.	All levels
Tolerance	Configured clock-skew tolerance, in seconds, for accepting keys for a key chain.	All levels
Id	Identification number configured for the current key.	detail

Table 72: show security keychain Output Fields (continued)

Field Name	Field Description	Level of Output
Algorithm	Authentication algorithm configured for the current key.	detail
State	<p>State of the current key.</p> <p>The value can be:</p> <ul style="list-style-type: none"> • receive • send • send-receive <p>For the active key, the State can be send-receive, send, or receive. For keys that have a future start time, the State is inactive. Compare the State field to the Mode field.</p>	detail
Option	<p>For IS-IS only, the option determines how Junos OS encodes the message authentication code in routing protocol packets.</p> <p>The values can be:</p> <ul style="list-style-type: none"> • basic—Based on RFC 5304. • isis-enhanced—Based on RFC 5310. <p>The default value is basic. When you configure the isis-enhanced option, Junos OS sends RFC 5310-encoded routing protocol packets and accepts both RFC 5304-encoded and RFC 5310-encoded routing protocol packets that are received from other devices.</p> <p>When you configure basic (or do not include the options statement in the key configuration) Junos OS sends and receives RFC 5304-encoded routing protocols packets, and drops 5310-encoded routing protocol packets that are received from other devices.</p> <p>Because this setting is for IS-IS only, the TCP and the BFD protocol ignore the encoding option configured in the key.</p>	detail
Start-time	Time that the current key became active.	detail
Mode	<p>Mode of each key (Informational only.)</p> <p>The value can be</p> <ul style="list-style-type: none"> • receive • send • send-receive <p>The mode of the key is based on the configuration. Suppose you configure two keys, one with a start-time of today and the other with a start-time of next week. For both keys, the Mode can be send-receive, send, or receive, regardless of the configured start-time. Compare the Mode field to the State field.</p>	detail

Sample Output

show security keychain brief

```
user@host> show security keychain brief
```

keychain	Active-ID		Next-ID		Transition	Tolerance
	Send	Receive	Send	Receive		
hakr	3	3	1	1	1d 23:58	3600

show security keychain detail

```
user@host> show security keychain detail
```

keychain	Active-ID		Next-ID		Transition	Tolerance
	Send	Receive	Send	Receive		
hakr	3	3	1	1	1d 23:58	3600
Id 3, Algorithm hmac-md5, State send-receive, Option basic						
Start-time Wed Aug 11 16:28:00 2010, Mode send-receive						
Id 1, Algorithm hmac-md5, State inactive, Option basic						
Start-time Fri Aug 20 11:30:57 2010, Mode send-receive						

show security macsec connections (MX Series)

Syntax	show security macsec connections <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers. Support for MPC7E-10G introduced in Junos OS Release 16.1R1 for MX240, MX480, and MX960 routers.
Description	Display the status of the active MACsec connections on the router.
Options	<p>none—Display MACsec connection information for all interfaces on the switch.</p> <p>interface <i>interface-name</i>—(Optional) Display MACsec connection information for the specified interface only.</p>
Required Privilege Level	view
List of Sample Output	show security macsec connections on page 1244 show security macsec connections (MX480 routers with MPC7E-10G) on page 1244 show security macsec connections (MX480 routers with MPC7E-10G) on page 1245
Output Fields	Table 40 on page 1092 lists the output fields for the show security macsec connections command. Output fields are listed in the approximate order in which they appear.

Table 73: show security macsec connections Output Fields

Field Name	Field Description
Fields for Interface	
Interface name	Name of the interface.
CA name	<p>Name of the connectivity association.</p> <p>A connectivity association is named using the connectivity-association statement when you are enabling MACsec.</p>
Cipher suite	Name of the cipher suite used for encryption.
Encryption	<p>Encryption setting. Encryption is enabled when this output is on and disabled when this output is off.</p> <p>The encryption setting is set using the no-encryption statement in the connectivity association when using static connectivity association key (CAK) security mode and is set using the encryption statement in the secure channel when using static secure association key (SAK) or dynamic security mode.</p>

Table 73: show security macsec connections Output Fields (continued)

Field Name	Field Description
Key server offset	<p>The offset value in a packet from which encryption can be performed.</p> <p>The offset is set using the offset statement when configuring the connectivity association when using static connectivity association key (CAK) or dynamic security mode or the secure channel when using static secure association key (SAK) security mode.</p>
Include SCI	<p>SCI tagging. The SCI tag is included on packets in a secure channel when this output is yes, and not included on packets in a secure channel when this output is no. SCI tagging is automatically enabled on MX Series routers.</p> <p>By default, include SCI tag is disabled. You can enable SCI tagging using the include-sci statement in the connectivity association configuration.</p>
Replay protect	<p>By default, replay protection is disabled. Replay protection ensures that a snooped packet is not replayed or a packet number is reused. Replay protection is enabled when this output is on and disabled when this output is off.</p> <p>You can enable replay protection using the replay-protect statement in the connectivity association configuration.</p>
Replay window	<p>Number of packets that can be replayed. Must be configured with replay protection. This output is set to 0 when replay protection is disabled, and is the size of the replay window, in number of packets, when replay protection is enabled.</p> <p>The size of the replay window is configured using the replay-window-size statement in the connectivity association configuration.</p>

Sample Output

show security macsec connections

```

user@host> show security macsec connections
Interface name: xe-0/1/0
  CA name: CA1
  Cipher suite: GCM-AES-128   Encryption: on
  Key server offset: 0        Include SCI: no
  Replay protect: off         Replay window: 0

```

show security macsec connections (MX480 routers with MPC7E-10G)

```

user@host> show security macsec connections
Interface name: xe-4/0/18
  CA name: ca1
  Cipher suite: GCM-AES-128   Encryption: on
  Key server offset: 30       Include SCI: no
  Replay protect: off         Replay window: 0
  Outbound secure channels
    SC Id: 54:1E:56:B4:0D:3A/1
    Outgoing packet number: 11
  Secure associations
    AN: 1 Status: inuse Create time: 1d 17:31:10

```



```
Inbound secure channels
  SC Id: 54:1E:56:B3:CA:A7/1
  Secure associations
    AN: 1 Status: inuse Create time: 1d 17:31:10
```

show security macsec connections (MX480 routers with MPC7E-10G)

```
user@host> show security macsec connections interface xe-1/0/7
```

```
CA name: caae1
  Cipher suite: AES_GCM_128   Encryption: off
  Key server offset: 0         Include SCI: no
  Replay protect: off         Replay window: 0
    Outbound secure channels
      SC Id: 54:1E:56:B3:CA:9C/1
      Outgoing packet number: 1
      Secure associations
        AN: 0 Status: inuse Create time: 4d 05:56:06
    Inbound secure channels
      SC Id: 54:1E:56:B4:0D:2F/1
      Secure associations
        AN: 0 Status: inuse Create time: 4d 05:56:06
```

show security macsec statistics

Syntax `show security macsec statistics`
`<brief | detail>`
`<interface interface-name>`

Release Information Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
 Command introduced in Junos OS Release 18.2R1 for ACX6360 Routers.

Description Display Media Access Control Security (MACsec) statistics.

This command does not display output when MACsec is enabled using static secure association key (SAK) security mode.

Options **none**—Display MACsec statistics in brief form for all interfaces on the switch.

brief | detail—(Optional) Display the specified level of output. Using the **brief** option is equivalent to entering the command with no options (the default). The **detail** option displays additional fields that are not visible in the **brief** output.



NOTE: The field names that only appear in this command output when you enter the **detail** option are mostly useful for debugging purposes by Juniper Networks support personnel.

interface interface-name—(Optional) Display MACsec statistics for the specified interface only.

Required Privilege Level view

Related Documentation • [show security macsec connections on page 1092](#)

List of Sample Output [show security macsec statistics interface xe-0/1/0 detail on page 1249](#)

Output Fields [Table 74 on page 1247](#) lists the output fields for the **show security macsec statistics** command. Output fields are listed in the approximate order in which they appear.

The field names that appear in this command output only when you enter the **detail** option are mostly useful for debugging purposes by Juniper Networks support personnel. Those field names are, therefore, not included in this table.

Table 74: show security macsec statistics Output Fields

Field Name	Field Description	Level of Output
Interface name	Name of the interface.	All levels
Fields for Secure Channel transmitted		
Encrypted packets	<p>Total number of packets transmitted out of the interface in the secure channel that were secured and encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>	All levels
Encrypted bytes	<p>Total number of bytes transmitted out of the interface in the secure channel that were secured and encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>	All levels
Protected packets	<p>Total number of packets transmitted out of the interface in the secure channel that were secured but not encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>	All levels
Protected bytes	<p>Total number of bytes transmitted out of the interface in the secure channel that were secured but not encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>	All levels
Fields for Secure Association transmitted		
Encrypted packets	<p>Total number of packets transmitted out of the interface in the connectivity association that were secured and encrypted using MACsec.</p> <p>The total includes the data packets transmitted in the secure channel and secured using a SAK and the control packets secured using a connectivity association key (CAK).</p>	All levels
Protected packets	<p>Total number of packets transmitted out of the interface in the connectivity association that were secured but not encrypted using MACsec.</p> <p>The total includes the data packets transmitted in the secure channel and secured using a SAK and the control packets secured using a connectivity association key (CAK).</p>	All levels
Fields for Secure Channel received		

Table 74: show security macsec statistics Output Fields (continued)

Field Name	Field Description	Level of Output
Accepted packets	<p>The number of received packets that have been accepted by the secure channel on the interface. The secure channel is used to send all data plane traffic on a MACsec-enabled link.</p> <p>A packet is considered accepted for this counter when it has been received by this interface and it has passed the MACsec integrity check.</p> <p>This counter increments for traffic that is and is not encrypted using MACsec.</p>	All levels
Validated bytes	<p>The number of bytes that have been validated by the MACsec integrity check and received on the secure channel on the interface. The secure channel is used to send all data plane traffic on a MACsec-enabled link.</p> <p>This counter does not increment when MACsec encryption is disabled.</p>	All levels
Decrypted bytes	<p>The number of bytes received in the secure channel on the interface that have been decrypted. The secure channel is used to send all data plane traffic on a MACsec-enabled link.</p> <p>An encrypted byte has to be decrypted before it can be received on the receiving interface. The decrypted bytes counter is incremented for received traffic that was encrypted using MACsec.</p>	All levels
Fields for Secure Association received		
Accepted packets	<p>The number of received packets that have been accepted in the connectivity association on the interface. The counter includes all control and data plane traffic accepted on the interface.</p> <p>A packet is considered accepted for this counter when it has been received by this interface and it has passed the MACsec integrity check.</p>	All levels
Validated bytes	<p>The number of bytes that have been validated by the MACsec integrity check and received on the connectivity association on the interface. The counter includes all control and data plane traffic accepted on the interface.</p> <p>This counter does not increment when MACsec encryption is disabled.</p>	All levels
Decrypted bytes	<p>The number of bytes received in the connectivity association on the interface that have been decrypted. The counter includes all control and data plane traffic accepted on the interface.</p> <p>An encrypted byte has to be decrypted before it can be received on the receiving interface. The decrypted bytes counter is incremented for received traffic that was encrypted using MACsec.</p>	All levels

Sample Output

show security macsec statistics interface xe-0/1/0 detail

```
user@host> show security macsec statistics interface xe-0/1/0 detail
```

```
Interface name: xe-0/1/0
Secure Channel transmitted
  Encrypted packets: 123858
  Encrypted bytes: 32190903
  Protected packets: 0
  Protected bytes: 0
Secure Association transmitted
  Encrypted packets: 123858
  Protected packets: 0
Secure Channel received
  Accepted packets: 123877
  Validated bytes: 0
  Decrypted bytes: 32196238
Secure Association received
  Accepted packets: 123877
  Validated bytes: 0
  Decrypted bytes: 32196238
Error and debug
Secure Channel transmitted packets
  Untagged: 0, Too long: 0
Secure Channel received packets
  Control: 0, Tagged miss: 3202804
  Untagged hit: 0, Untagged: 0
  No tag: 0, Bad tag: 0
  Unknown SCI: 0, No SCI: 0
  Control pass: 0, Control drop: 0
  Uncontrol pass: 123877, Uncontrol drop: 0
  Hit dropped: 0, Invalid accept: 0
  Late drop: 0, Delayed accept: 0
  Unchecked: 0, Not valid drop: 0
  Not using SA drop: 0, Unused SA accept: 0
```

include-sci (MACsec for MX Series)

Syntax	include-sci;
Hierarchy Level	[edit security macsec connectivity-association <i>connectivity-association-name</i>]
Release Information	Statement introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers.
Description	<p>Specifies that the SCI tag should be appended to each packet on a link that has enabled MACsec.</p> <p>This option is used only when connecting a router to a host device that requires SCI tagging. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.</p>
Default	SCI tagging is not enabled by default.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Media Access Control Security (MACsec) on MX Series Routers on page 268

show security mka sessions

Syntax	show security mka sessions <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Command introduced in Junos OS Release 18.2R1 for ACX6360 Routers. Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.
Description	Display MACsec Key Agreement (MKA) session information.
Options	<ul style="list-style-type: none"> interface <i>interface-name</i>—(Optional) Display the MKA session information for the specified interface only.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> show security mka statistics on page 1258 show security macsec connections on page 1092 show security macsec statistics on page 1246
List of Sample Output	show security mka sessions on page 1252
Output Fields	Table 75 on page 1251 lists the output fields for the show security mka sessions command. Output fields are listed in the approximate order in which they appear.

Table 75: show security mka sessions Output Fields

Field Name	Field Description
Interface name	Name of the interface.
Member identifier	Name of the member identifier.
CAK name	Name of the Connectivity Association Key (CAK). The CAK is configured using the cak keyword when configuring the pre-shared key.
Transmit interval	The transmit interval.
Outbound SCI	Name of the outbound secure channel identifier.
Message number	Number of the last data message.
Key number	Key number.

Table 75: show security mka sessions Output Fields (continued)

Field Name	Field Description
Key server	Key server status. The switch is the key server when this output is yes . The switch is not the key server when this output is no .
Key server priority	The key server priority. The key server priority can be set using the key-server-priority statement.
Latest SAK AN	Name of the latest secure association key (SAK) association number.
Latest SAK KI	Name of the latest secure association key (SAK) key identifier.
Fields for Peer list	
Member identifier	Name of the member identifier.
Hold time	Hold time, in seconds.
Message number	Number of the last data message
SCI	Name of the secure channel identifier.
Lowest acceptable PN	Number of the lowest acceptable packet number (PN).

Sample Output

show security mka sessions

```
user@host> show security mka sessions
```

```
Interface name: xe-0/1/0
  Member identifier: OCCBEE42F8778300F8D0C1DC
  CAK name: 1234567890
  Transmit interval: 2000(ms)
  Outbound SCI: 2C:6B:F5:9D:4B:1B/1
  Message number: 1526465      Key number: 0
  Key server: no              Key server priority: 15
  Latest SAK AN: 0            Latest SAK KI: 4F18CE25228178FD15976E4C/1
  Previous SAK AN: 0          Previous SAK KI: 000000000000000000000000/0
  Peer list
    1. Member identifier: 4F18CE25228178FD15976E4C (live)
      Message number: 1526484 Hold time: 14500 (ms)
      SCI: 2C:6B:F5:9D:3A:1B/1
      Lowest acceptable PN: 121198
```


show security mka sessions (MX Series)

Syntax	show security mka sessions <interface <i>interface-name</i> > <summary brief detail>
Release Information	Command introduced in Junos OS Release 15.1 for MX240, MX480, and MX960 routers. Support for MPC7E-10G introduced in Junos OS Release 16.1R1 for MX240, MX480, and MX960 routers.
Description	Display MACsec Key Agreement (MKA) session information for all interfaces. The MKA protocol is responsible for maintaining MACsec on the link, and decides which router on the point-to-point link becomes the key server.
Options	<ul style="list-style-type: none"> • interface<i>interface-name</i>—Display the MKA session information for the specified interface only. • summary brief detail—Display the specified level of output. • none (same as brief)—Display the MKA session information for all interfaces.
Required Privilege Level	view
List of Sample Output	show security mka sessions on page 1255 show security mka sessions (MX480 with MPC7E-10G) on page 1255 show security mka sessions (MX480 with MPC7E-10G) on page 1255 show security mka sessions detail on page 1256
Output Fields	Table 75 on page 1251 lists the output fields for the show security mka sessions command. Output fields are listed in the approximate order in which they appear.

Table 76: show security mka sessions Output Fields

Field Name	Field Description
Interface name	Name of the interface.
Interface state	Shows whether the interface is secured or not. If it is secured, the CAK type is also displayed.
Member identifier	Name of the member identifier.
CAK name	Name of the connectivity association key (CAK). The CAK is configured using the cak keyword when configuring the pre-shared key.
CAK type	The CAK type: primary, fallback, or preceding.

Table 76: show security mka sessions Output Fields (continued)

Field Name	Field Description
Transmit interval	The transmit interval. Both ends of the point-to-point link should be configured to the same value. Default value is 2000 seconds. Possible values: 2000 through 6000 milliseconds.
Outbound SCI	Name of the outbound secure channel identifier.
Message number	Number of the last data message.
Key number	Key number.
Key server	Key server status. The router is the key server when this output is yes . The router is not the key server when this output is no .
Key server priority	Displays the priority of the key server. Lower value indicates higher priority. Use the key-server-priority statement to set the priority. Possible values: 0 through 255.
Latest SAK AN	Name of the latest secure association key (SAK) association number.
Latest SAK KI	Name of the latest secure association key (SAK) key identifier.
Fields for Peer list	
Member identifier	Name of the member identifier.
Hold time	Hold time, in seconds.
Message number	Number of the last data message
SCI	Name of the secure channel identifier.
Lowest acceptable PN	Number of the lowest acceptable packet number (PN).
Fields for CAK list (detail only)	
CAK name	Name of the connectivity association key (CAK).
CAK type	The CAK type: primary, fallback, or preceding.
Status	The CAK status: live, active, or in-progress.
Member identifier	Name of the member identifier.
Message number	Number of the last data message

Sample Output

show security mka sessions

```
user@host> show security mka sessions
```

```
Interface name: xe-0/1/0
  Member identifier: 0CCBEE42F8778300F8D0C1DC
  CAK name: 1234567890
  Transmit interval: 2000(ms)
  Outbound SCI: 2C:6B:F5:9D:4B:1B/1
  Message number: 1526465      Key number: 0
  Key server: no              Key server priority: 15
  Latest SAK AN: 0            Latest SAK KI: 4F18CE25228178FD15976E4C/1
  Previous SAK AN: 0          Previous SAK KI: 0000000000000000000000/0
  Peer list
    1. Member identifier: 4F18CE25228178FD15976E4C (live)
      Message number: 1526484 Hold time: 14500 (ms)
      SCI: 2C:6B:F5:9D:3A:1B/1
      Lowest acceptable PN: 121198
```

show security mka sessions (MX480 with MPC7E-10G)

```
user@host> show security mka sessions
```

```
Interface name: xe-4/0/18
  Member identifier: FA606FD4A4C2172F0C9D9C1F
  CAK name: ABCDEF
  Transmit interval: 2000(ms)
  Outbound SCI: 54:1E:56:B4:0D:3A/1
  Message number: 72455      Key number: 0
  Key server: no              Key server priority: 16
  Latest SAK AN: 1            Latest SAK KI: 88EC3950C7D598623A406AC8/2
  Previous SAK AN: 0          Previous SAK KI: 0000000000000000000000/0
  Peer list
    1. Member identifier: 88EC3950C7D598623A406AC8 (live)
      Message number: 72552 Hold time: 4500 (ms)
      SCI: 54:1E:56:B3:CA:A7/1
      Lowest acceptable PN: 0
```

show security mka sessions (MX480 with MPC7E-10G)

```
user@host> show security mka sessions interface xe-1/0/7
```

```
Member identifier: 653D8911B42DAE946993B40F
  CAK name: 1111
  Transmit interval: 2000(ms)
  Outbound SCI: 54:1E:56:B3:CA:9C/1
  Message number: 179139      Key number: 0
  Key server: no              Key server priority: 16
  Latest SAK AN: 0            Latest SAK KI: 64EF352178BD1833600338F9/1
  Previous SAK AN: 0          Previous SAK KI: 0000000000000000000000/0
  Peer list
    1. Member identifier: 64EF352178BD1833600338F9 (live)
      Message number: 179175 Hold time: 4500 (ms)
      SCI: 54:1E:56:B4:0D:2F/1
      Lowest acceptable PN: 0
```

show security mka sessions detail

```
user@host> show security mka sessions detail
```

```
Interface name: xe-0/1/0
Interface state: Secured - Preceding
Member identifier: OCCBEE42F8778300F8D0C1DC
CAK name: 8888
CAK type: preceding
Transmit interval: 2000(ms)
Outbound SCI: 2C:6B:F5:9D:4B:1B/1
Message number: 1526465      Key number: 1
Key server: no              Key server priority: 16
Latest SAK AN: 1            Latest SAK KI: 4F18CE25228178FD15976E4C/1
Previous SAK AN: 0          Previous SAK KI: 0000000000000000000000/0
CAK list: (3)
  1. CAK name: 8888
     CAK type: preceding                      Status: live
     Member identifier: E752CAEAE8DDFB82D4EA4BF7 Message number: 8880
     Peer list: (1)
       1. Member identifier: 920A4EE089DEE5FCC7B7330E (live)
          Message number: 8943      Hold time: 5000 (ms)
          SCI: 2C:6B:F5:9D:3A:1B/1
          Lowest acceptable PN: 0
  2. CAK name: FFFF
     CAK type: fallback                      Status: active
     Member identifier: 8F2D5171F38EAB16C2E0CB62 Message number: 8951
     Peer list: (1)
       1. Member identifier: E0014FB5F890936DFC4FECC3 (live)
          Message number: 8944      Hold time: 5000 (ms)
          SCI: 88:E0:F3:1F:40:64/1
          Lowest acceptable PN: 0
  3. CAK name: AAAA
     CAK type: primary                      Status: in-progress
     Member identifier: 920A4EE089DEE5FCC7B7330E Message number: 2431
     Peer list: (0)
```

show security mka sessions summary

Syntax `show security mka sessions summary`

Release Information Command introduced in Junos OS Release 19.2 for MX Series routers.

Description Display MACsec Key Agreement (MKA) session information to see the number of MKAs that are in progress, connectivity association key (CAK) type, CAK status, and MKA packet count activity.

Required Privilege Level view

List of Sample Output [show security mka sessions summary on page 1257](#)

Output Fields [Table 77 on page 1257](#) lists the output fields for the `show security mka sessions summary` command. Output fields are listed in the approximate order in which they appear.

Table 77: show security mka sessions summary Output Fields

Field Name	Field Description
Interface name	Name of the interface.
Member ID	Member identifier.
Type	The CAK type: primary, fallback, or preceding.
Status	The CAK status: live, active, or in-progress.
Tx	MKA packets transmitted on the interface.
Rx	MKA packets received on the interface.
CAK name	Name of the connectivity association key (CAK). The CAK is configured using the <code>cak</code> keyword when configuring the pre-shared key.

Sample Output

show security mka sessions summary

```
user@host> show security mka sessions summary
```

```
Interface  Member-ID          Type   Status  Tx  Rx  CAK Name
ge-0/0/1   E752CAEAE8DDFB82D4EA4BF7 preceding live   8887 8951 8888
ge-0/0/1   0F2D5171F38EAB16C2E0CB62 fallback active  8959 8952 FFFF
ge-0/0/1   6B49BD5CF7188F3CD9A29D30 primary  in-progress 2439 0  AAAA
```

show security mka statistics

Syntax	<code>show security mka statistics</code> <code><interface <i>interface-name</i>></code>
Release Information	Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Command introduced in Junos OS Release 18.2R1 for ACX6360 routers.
Description	Display MACsec Key Agreement (MKA) protocol statistics. The output for this command does not include statistics for MACsec data traffic. For MACsec data traffic statistics, see show security macsec statistics .
Options	<ul style="list-style-type: none"> interface <i>interface-name</i>—(Optional) Display the MKA information for the specified interface only.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> show security mka sessions on page 1251 show security macsec statistics on page 1246 show security macsec connections on page 1092
List of Sample Output	show security mka statistics on page 1259
Output Fields	Table 78 on page 1258 lists the output fields for the show security mka statistics command. Output fields are listed in the approximate order in which they appear.

Table 78: show security mka statistics Output Fields

Field Name	Field Description
Received packets	<p>Number of received MKA control packets.</p> <p>This counter increments for received MKA control packets only. This counter does not increment when data packets are received.</p>
Transmitted packets	<p>Number of transmitted MKA packets</p> <p>This counter increments for transmitted MKA control packets only. This counter does not increment when data packets are transmitted.</p>
Version mismatch packets	Number of version mismatch packets.

Table 78: show security mka statistics Output Fields (continued)

Field Name	Field Description
CAK mismatch packets	Number of Connectivity Association Key (CAK) mismatch packets. This counter increments when the connectivity association key (CAK) and connectivity association key name (CKN), which are user-configured values that have to match to enable MACsec, do not match for an MKA control packet.
ICV mismatch packets	Number of ICV mismatched packets. This counter increments when the connectivity association key (CAK) value does not match on both ends of a MACsec-secured Ethernet link.
Duplicate message identifier packets	Number of duplicate message identifier packets.
Duplicate message number packets	Number of duplicate message number packets.
Duplicate address packets	Number of duplicate source MAC address packets.
Invalid destination address packets	Number of invalid destination MAC address packets.
Formatting error packets	Number of formatting error packets.
Old Replayed message number packets	Number of old replayed message number packets.

Sample Output

show security mka statistics

```
user@host> show security mka statistics
```

```

Received packets:          1525844
Transmitted packets:       1525841
Version mismatch packets:  0
CAK mismatch packets:      0
ICV mismatch packets:      0
Duplicate message identifier packets: 0
Duplicate message number packets: 0
Duplicate address packets:  0
Invalid destination address packets: 0
Formatting error packets:   0
Old Replayed message number packets: 0
```

show security pki ca-certificate

Syntax `show security pki ca-certificate
<brief | detail>
<ca-profile ca-profile-name>`

Release Information Command introduced in Junos OS Release 7.5.

Description Display information about certificate authority (CA) digital certificates installed in the router.

Options **none**—(Same as brief) Display information about all CA digital certificates.

brief | detail—(Optional) Display the specified level of output.

ca-profile *ca-profile-name*—(Optional) Display information about only the specified CA profile.

Required Privilege Level view

List of Sample Output [show security pki ca-certificate on page 1261](#)
[show security pki ca-certificate detail on page 1262](#)

Output Fields [Table 79 on page 1260](#) lists the output fields for the **show security pki ca-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 79: show security pki ca-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	detail
Serial number	Unique serial number of the digital certificate.	detail
Issued by	Authority that issued the digital certificate.	none brief
Issued to	Device that was issued the digital certificate.	none brief

Table 79: show security pki ca-certificate Output Fields (continued)

Field Name	Field Description	Level of Output
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the authority. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the requestor. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail
Validity	Time period when the digital certificate is valid. Values are: <ul style="list-style-type: none"> • Not before—Start time when the digital certificate becomes valid. • Not after—End time when the digital certificate becomes invalid. 	All levels
Public key algorithm	Encryption algorithm used with the private key, such as rsaEncryption(1024 bits) .	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption .	detail
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	detail
Distribution CRL	Distinguished name information and the URL for the certificate revocation list (CRL) server.	detail
Use for key	Use of the public key, such as Certificate signing , CRL signing , Digital signature , or Key encipherment .	detail

Sample Output

show security pki ca-certificate

```

user@host> show security pki ca-certificate
Certificate identifier: abc
Issued to: example, Issued by: example
Validity:
  Not before: 2005 Oct 18th, 23:54:22 GMT
  Not after: 2025 Oct 19th, 00:24:22 GMT
Public key algorithm: rsaEncryption(1024 bits)

```

```

Certificate identifier: entrust
  Issued to: First Officer, Issued by: example
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)

```

```

Certificate identifier:abe
  Issued to: First Officer, Issued by: example
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)

```

show security pki ca-certificate detail

```
user@host> show security pki ca-certificate detail
```

```

Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 9235
  Issuer:
    Organization: example, Country: us
  Subject:
    Organization: example, Country: us
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
    0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
    78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
    19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
    bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
    c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
    04:47:08:07:de:17:23:13
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
    71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
  Distribution CRL:
    C=us, O=example, CN=CRL1
    http://CA-1/CRL/example_us_crlfile.crl
  Use for key: CRL signing, Certificate signing
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925c
  Issuer:
    Organization: example, Country: us
  Subject:
    Organization: example, Country: us, Common name: First Officer
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
    1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
    34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
    19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a

```

```

ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
da:eb:10:27:bd:46:34:33
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
  23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
Distribution CRL:
  C=us, O=example, CN=CRL1
  http://CA-1/CRL/example_us_crlfile.crl
Use for key: Key encipherment
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925b
Issuer:
  Organization: example, Country: us
Subject:
  Organization: example, Country: us, Common name: First Officer
Validity:
  Not before: 2005 Oct 18th, 23:55:59 GMT
  Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
af:44:bf:53:aa:d4:5f:67
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
  ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
Distribution CRL:
  C=us, O=example, CN=CRL1
  http://CA-1/CRL/example_us_crlfile.crl
Use for key: Digital signature

```

show security pki certificate-request

Syntax `show security pki certificate-request
<brief | detail>
<certificate-id certificate-id-name>`

Release Information Command introduced in Junos OS Release 7.5.

Description Display information about manually generated local digital certificate requests that are stored in the router.

Options **none**—(same as brief) Display information about all local digital certificate requests.

brief | detail—(Optional) Display the specified level of output.

certificate-id *certificate-id-name*—(Optional) Display information about only the specified local digital certificate request

Required Privilege Level view

Related Documentation

- [clear security pki certificate-request on page 1071](#)

List of Sample Output [show security pki certificate-request on page 1265](#)
[show security pki certificate-request detail on page 1265](#)

Output Fields [Table 80 on page 1264](#) lists the output fields for the **show security pki certificate-request** command. Output fields are listed in the approximate order in which they appear.

Table 80: show security pki certificate-request Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	detail
Issued to	Device that was issued the digital certificate.	none brief
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the authority. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail

Table 80: show security pki certificate-request Output Fields (continued)

Field Name	Field Description	Level of Output
Alternate subject	Domain name or IP address of the device related to the digital certificate.	detail
Validity	Time period when the digital certificate is valid. Values are: <ul style="list-style-type: none"> • Not before—Time when the digital certificate becomes valid. • Not after—End time when the digital certificate becomes invalid. 	All levels
Public key algorithm	Encryption algorithm used with the private key, such as rsaEncryption(1024 bits) .	All levels
Public key verification status	Public key verification status: Failed or Passed . The detail output also provides the verification hash.	All levels
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	detail
Use for key	Use of the public key, such as Certificate signing , CRL signing , Digital signature , or Key encipherment .	detail

Sample Output

show security pki certificate-request

```

user@host> show security pki certificate-request
Certificate identifier: local-microsoft-2
Issued to: router2.example.com
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed

```

show security pki certificate-request detail

```

user@host> show security pki certificate-request detail
Certificate identifier: local-entrust3
Certificate version: 3
Subject:
  Common name: router3.example.com
Alternate subject: router3.example.com
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
  fb:79:df:d4:a9:03:0f:d3:69:7e:c1:e4:27:35:9c:d9:b1:a2:47:78
  d2:6d:f3:e5:f4:68:4f:b3:04:45:88:57:99:82:39:a6:51:9e:5f:42
  23:3f:d7:6e:3d:a5:54:a9:b1:2d:6e:90:dd:12:8a:bf:ef:2b:20:50
  ba:f0:da:d9:0c:ad:5e:d6:c6:98:3a:ae:3f:90:dd:94:78:c1:ea:2e
  7c:f0:2d:d4:79:d4:cd:f0:52:df:5e:72:f2:e7:ae:66:f7:61:f4:bc
  72:57:3e:6c:6d:d3:24:58:8b:f4:ef:da:2a:6a:fa:eb:98:f8:34:84
  79:54:da:4f:d3:6f:52:1f
Fingerprint:
  7c:e8:f9:45:93:8d:a3:92:7f:18:29:02:f1:c8:e2:85:3d:ad:df:1f (sha1)
  00:4e:df:a0:6b:ad:8c:50:da:7c:a1:cf:5d:37:b0:ea (md5)
Use for key: Digital signature

```


show security pki crt

Syntax `show security pki crt
<brief | detail>
<ca-profile ca-profile-name>`

Release Information Command introduced in Junos OS Release 8.1.

Description Display information about the certificate revocation lists (CRLs) that are stored in the router.

Options **none**—(same as brief) Display information about all CRLs.

brief | detail—(Optional) Display the specified level of output.

ca-profile ca-profile-name—(Optional) Display CRL information about only the specified CA profile.

Required Privilege Level view

Related Documentation

- [clear security pki crt on page 1097](#)

List of Sample Output [show security pki crt on page 1268](#)
[show security pki crt detail on page 1268](#)

Output Fields [Table 81 on page 1267](#) shows the output fields for the **show security pki crt** command. Output fields are listed in the approximate order in which they appear.

Table 81: show security pki crt Output Fields

Field Name	Field Description	Level of Output
CA profile	Name of the configured CA profile.	All levels
CRL version	Revision number of the certificate revocation list.	All levels
CRL number	Number of the certificate revocation list	All levels
CRL Issuer	Device that was issued the certificate revocation list.	All levels

Table 81: show security pki crl Output Fields (continued)

Field Name	Field Description	Level of Output
Issuer	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the authority. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail
Effective date	Date and time the certificate revocation list becomes valid.	All levels
Next update	Date and time the router will download the latest version of the certificate revocation list.	All levels
Revocation List	List of digital certificates that have been revoked before their expiration date. Values are: <ul style="list-style-type: none"> • Serial number—Unique serial number of the digital certificate • Revocation date—Date and time that the digital certificate was revoked. 	detail

Sample Output

show security pki crl

```
user@host> show security pki crl
CA profile entrust
CRL version: V2
CRL number: 24
CRL issuer: C=CA, O=juniper
Effective date: 2006 May 31st, 05:35:25 GMT
Next update: 2006 Jun 1st, 06:35:25 GMT
```

show security pki crl detail

```
user@host> show security pki crl detail
CA profile: entrust
CRL version: V2
CRL number: 24
Issuer:
Organization: juniper, Country: ca
Validity:
Effective date: 2006 May 31st, 05:35:25 GMT
Next update: 2006 Jun 1st, 06:35:25 GMT
Revocation List:
Serial number      Revocation date
4451aca3 2006      May 25th, 09:13:38 GMT
4451aca4 2006      May 25th, 10:11:33 GMT
4451acb4 2006      May 29th, 11:28:54 GMT
4451aceb 2006      May 29th, 11:29:01 GMT
```


4451acfe 2006	May 29th, 11:29:17 GMT
4451acff 2006	May 31st, 05:29:55 GMT

show security pki local-certificate

Syntax show security pki local-certificate
<brief | detail>
<certificate-id *certificate-id-name*>
<system-generated>

Release Information Command introduced in Junos OS Release 7.5.

Description Display information about the local digital certificates and the corresponding public keys installed in the router.

Options **none**—(same as brief) Display information about all local digital certificates and corresponding public keys.

brief | detail—(Optional) Display the specified level of output.

certificate-id *certificate-id-name*—(Optional) Display information about only the specified the local digital certificate and corresponding public keys.

system-generated—(Optional) Auto-generated self-signed certificate.

Required Privilege Level view

Related Documentation [• clear security pki local-certificate on page 1099](#)

List of Sample Output [show security pki local-certificate on page 1271](#)
[show security pki local-certificate detail on page 1272](#)

Output Fields [Table 82 on page 1270](#) lists the output fields for the **show security pki local-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 82: show security pki local-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	detail
Serial number	Unique serial number of the digital certificate.	detail
Issued by	Authority that issued the digital certificate.	none brief
Issued to	Device that was issued the digital certificate.	none brief

Table 82: show security pki local-certificate Output Fields (continued)

Field Name	Field Description	Level of Output
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the authority. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the authority. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail
Alternate subject	Domain name or IP address of the device related to the digital certificate.	detail
Validity	Time period when the digital certificate is valid. Values are: <ul style="list-style-type: none"> • Not before—Start time when the digital certificate becomes valid. • Not after—End time when the digital certificate becomes invalid. 	All levels
Public key algorithm	Encryption algorithm used with the private key, such as rsaEncryption (1024 bits) .	All levels
Public key verification status	Public key verification status: Failed or Passed . The detail output also provides the verification hash.	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption .	detail
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	detail
Distribution CRL	Distinguished name information and URL for the certificate revocation list (CRL) server.	detail
Use for key	Use of the public key, such as Certificate signing , CRL signing , Digital signature , or Key encipherment .	detail

Sample Output

show security pki local-certificate

```
user@host> show security pki local-certificate
```

```
Certificate identifier: local-entrust2
Issued to: router2.example.com, Issued by: juniper
Validity:
  Not before: 2005 Nov 21st, 23:28:22 GMT
  Not after: 2008 Nov 21st, 23:58:22 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
```

show security pki local-certificate detail

```
user@host> show security pki local-certificate detail

Certificate identifier: local-entrust3
Certificate version: 3
Serial number: 4355 94f9
Issuer:
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us, Common name: router3.example.com
Alternate subject: router3.example.com
Validity:
  Not before: 2005 Nov 21st, 23:33:58 GMT
  Not after: 2008 Nov 22nd, 00:03:58 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
fb:79:df:d4:a9:03:0f:d3:69:7e:c1:e4:27:35:9c:d9:b1:a2:47:78
d2:6d:f3:e5:f4:68:4f:b3:04:45:88:57:99:82:39:a6:51:9e:5f:42
23:3f:d7:6e:3d:a5:54:a9:b1:2d:6e:90:dd:12:8a:bf:ef:2b:20:50
ba:f0:da:d9:0c:ad:5e:d6:c6:98:3a:ae:3f:90:dd:94:78:c1:ea:2e
7c:f0:2d:d4:79:d4:cd:f0:52:df:5e:72:f2:e7:ae:66:f7:61:f4:bc
72:57:3e:6c:6d:d3:24:58:8b:f4:ef:da:2a:6a:fa:eb:98:f8:34:84
79:54:da:4f:d3:6f:52:1f
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  61:3a:d0:b4:7a:16:9b:39:ba:81:3f:9d:ab:34:e5:c8:be:3b:a1:6d (sha1)
  60:a0:ff:58:05:4a:65:73:9d:74:3a:e1:83:6f:1b:c8 (md5)
Distribution CRL:
  C=us, O=juniper, CN=CRL1
  http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Digital signature
```

show services ipsec-vpn certificates

Syntax `show services ipsec-vpn certificates`
`<brief | detail>`
`<service-set service-set>`

Release Information Command introduced in Junos OS Release 7.5.

Description (Adaptive services interfaces only) Display local and remote certificates installed in the IPsec configuration memory cache that are used for the IKE negotiation.

Options **none**—(same as brief) Display information about local and remote certificates associated with all service sets.

brief | detail—(Optional) Display the specified level of output.

service-set service-set—(Optional) Display information about local and remote certificates associated with only the specified service set.

Required Privilege Level view

List of Sample Output [show services ipsec-vpn certificates on page 1274](#)
[show security ipsec-vpn certificates detail on page 1275](#)

Output Fields [Table 83 on page 1273](#) lists the output fields for the **show services ipsec-vpn certificates** command. Output fields are listed in the approximate order in which they appear.

Table 83: show services ipsec-vpn certificates Output Fields

Field Name	Field Description	Level of Output
Service set	Name of the IPsec service set.	All levels
Total entries	Number of certificate cache entries.	All levels
Certificate cache entry	Identification number of the certificate cache entry.	All levels
Flags	Information about the digital certificate, including whether the certificate is a root certificate and trusted.	none brief
Issued to	Device that was issued the digital certificate.	none brief
Issued by	Authority that issued the digital certificate.	none brief
Certificate version	Revision number of the digital certificate.	detail

Table 83: show services ipsec-vpn certificates Output Fields (continued)

Field Name	Field Description	Level of Output
Serial number	Unique serial number of the digital certificate.	detail
Alternate subject	Domain name or IP address of the device related to the digital certificate.	All levels
Validity	Time period when the digital certificate is valid. Values are: <ul style="list-style-type: none"> • Not before—Start time when the digital certificate becomes valid. • Not after—End time when the digital certificate becomes invalid. 	none brief
Public key algorithm	Specifies the encryption algorithm used with the private key, such as rsaEncryption (1024 bits) .	detail
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption .	detail
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	detail
Distribution CRL	Distinguished name information and the URL for the certificate revocation list (CRL) server.	detail
Use for key	Use of the public key, such as Certificate signing , CRL signing , Digital signature , or Key encipherment .	detail

Sample Output

show services ipsec-vpn certificates

```

user@host> show services ipsec-vpn certificates
Service set: serviceset-dynamic-BiEspsha3des, Total entries: 3
Certificate cache entry: 3
  Flags: Non-root Trusted
  Issued to: router3.example.com, Issued by: juniper
  Alternate subject: router3.example.com
  Validity:
    Not before: 2005 Nov 21st, 23:33:58 GMT
    Not after: 2008 Nov 22nd, 00:03:58 GMT

Certificate cache entry: 2
  Flags: Non-root Trusted
  Issued to: router2.example.com, Issued by: juniper
  Alternate subject: router2.example.com
  Validity:
    Not before: 2005 Nov 21st, 23:28:22 GMT
    Not after: 2008 Nov 21st, 23:58:22 GMT

Certificate cache entry: 1
  Flags: Root Trusted
  Issued to: juniper, Issued by: juniper
  Validity:

```

```
Not before: 2005 Oct 18th, 23:54:22 GMT
Not after: 2025 Oct 19th, 00:24:22 GMT
```

show security ipsec-vpn certificates detail

```
user@host> show services ipsec-vpn certificates detail
```

```
Service set: serviceset-dynamic-BiEspsha3des, Total entries: 3
```

```
Certificate cache entry: 3
```

```
Certificate version: 3
```

```
Serial number: 4355 94f9
```

```
Alternate subject: router3.example.com
```

```
Public key algorithm: rsaEncryption
```

```
Signature algorithm: sha1WithRSAEncryption
```

```
Fingerprint:
```

```
61:3a:d0:b4:7a:16:9b:39:ba:81:3f:9d:ab:34:e5:c8:be:3b:a1:6d (sha1)
```

```
60:a0:ff:58:05:4a:65:73:9d:74:3a:e1:83:6f:1b:c8 (md5)
```

```
Distribution CRL:
```

```
C=us, O=juniper, CN=CRL1
```

```
http://CA-1/CRL/juniper_us_crlfile.crl
```

```
Use for key: Digital signature
```

```
Certificate cache entry: 2
```

```
Certificate version: 3
```

```
Serial number: 4355 94f8
```

```
Alternate subject: router2.example.com
```

```
Public key algorithm: rsaEncryption
```

```
Signature algorithm: sha1WithRSAEncryption
```

```
Fingerprint:
```

```
30:c3:a4:04:da:33:9d:60:23:5a:48:75:48:2c:f0:c6:96:6c:31:fa (sha1)
```

```
9a:a2:ce:ef:7e:10:80:a0:c8:4d:2f:e7:e1:d3:69:9d (md5)
```

```
Distribution CRL:
```

```
C=us, O=juniper, CN=CRL1
```

```
http://CA-1/CRL/juniper_us_crlfile.crl
```

```
Use for key: Digital signature
```

```
Certificate cache entry: 1
```

```
Certificate version: 3
```

```
Flags: Root
```

```
Serial number: 4355 9235
```

```
Public key algorithm: rsaEncryption
```

```
Signature algorithm: sha1WithRSAEncryption
```

```
Fingerprint:
```

```
00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
```

```
71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
```

```
Distribution CRL:
```

```
C=us, O=juniper, CN=CRL1
```

```
http://CA-1/CRL/juniper_us_crlfile.crl
```

```
Use for key: CRL signing, Certificate signing
```

show services ipsec-vpn ike security-associations

Syntax `show services ipsec-vpn ike security-associations
<brief | detail>
<peer-address>`

Release Information Command introduced before Junos OS Release 7.4.
Statistics for Internet Key Exchange (IKE) security associations for each services PIC introduced in Junos OS Release 12.1.

Description (Adaptive services interface only) Display information for Internet Key Exchange (IKE) security associations. If no security association is specified, the information for all security associations is displayed.

Options **none**—(same as brief) Display standard information for all IPsec security associations.
brief | detail—(Optional) Display the specified level of output.
peer-address—(Optional) Display information about a particular security association address.

Required Privilege Level view

List of Sample Output [show services ipsec-vpn ike security-associations on page 1278](#)
[show services ipsec-vpn ike security-associations detail on page 1279](#)
[show services ipsec-vpn ike security-associations \(on ACX500 Routers\) on page 1280](#)

Output Fields [Table 84 on page 1276](#) lists the output fields for the **show services ipsec-vpn ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 84: show services ipsec-vpn ike security-associations Output Fields

Field Name	Field Description	Level of Output
IKE peer	Remote end of the IKE negotiation.	detail
Role	Part played in the IKE session. The router triggering the IKE negotiation is the initiator, and the router accepting the first IKE exchange packets is the responder.	detail
Remote Address	Responder's address.	none specified
State	State of the IKE security association: <ul style="list-style-type: none"> • Matured—IKE security association is established. • Not matured—The IKE security association is in the process of negotiation. 	none specified

Table 84: show services ipsec-vpn ike security-associations Output Fields (continued)

Field Name	Field Description	Level of Output
Initiator cookie	When the IKE negotiation is triggered, a random number is sent to the remote node.	All levels
Responder cookie	<p>The remote node generates its own random number and sends it back to the initiator as a verification that the packets were received.</p> <p>Of the numerous security services available, protection against denial of service (DoS) is one of the most difficult to address. A “cookie” or anticlogging token (ACT) is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie’s authenticity. An exchange prior to CPU-intensive public key operations can thwart some DoS attempts (such as simple flooding with invalid IP source addresses).</p>	All levels
Exchange type	<p>Specifies the number of messages in an IKE exchange, and the payload types that are contained in each message. Each exchange type provides a particular set of security services, such as anonymity of the participants, perfect forward secrecy of the keying material, and authentication of the participants. Junos OS supports two types of exchanges:</p> <ul style="list-style-type: none"> • Main—The exchange is done with six messages. Main encrypts the payload, protecting the identity of the neighbor. • Aggressive—The exchange is done with three messages. Aggressive does not encrypt the payload, leaving the identity of the neighbor unprotected. • IKEv2—The exchange is negotiated using IKE version 2. 	All levels
PIC	The services PIC for which the IKE security associations are displayed.	All levels
Authentication method	<p>Authentication method that determines which payloads are exchanged and when they are exchanged. Value can be ECDSA-signatures (256 bit key), ECDSA-signatures (384 bit key), Pre-shared-keys, or RSA-signatures.</p> <p>NOTE: In Junos FIPS mode, ECDSA is not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, ECDSA is supported in Junos FIPS mode.</p>	detail
Local	Prefix and port number of the local end.	detail
Remote	Prefix and port number of the remote end.	detail
Lifetime	Number of seconds remaining until the IKE security association expires.	detail
Algorithms	<p>Header for the IKE algorithms output.</p> <ul style="list-style-type: none"> • Authentication—(detail output only) Type of authentication algorithm used: md5 or sha1 • Encryption—(detail output only) Type of encryption algorithm used: des-cbc, 3des-cbc, or None. • Pseudo random function—Function that generates highly unpredictable random numbers: hmac-md5 or hmac-sha1. 	detail

Table 84: show services ipsec-vpn ike security-associations Output Fields (continued)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Number of bytes and packets received and transmitted on the IKE security association.</p> <ul style="list-style-type: none"> Input bytes, Output bytes—Number of bytes received and transmitted on the IKE security association. Input packets, Output packets—Number of packets received and transmitted on the IKE security association. 	detail
Flags	<p>Notification to the key management process of the status of the IKE negotiation:</p> <ul style="list-style-type: none"> caller notification sent—Caller program notified about the completion of the IKE negotiation. waiting for done—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. waiting for remove—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. waiting for policy manager—Negotiation is waiting for a response from the policy manager. 	detail
IPsec security associates	<p>Number of IPsec security associations created and deleted with this IKE security association.</p>	detail
Phase 2 negotiations in progress	<p>Number of phase 2 negotiations in progress and status information:</p> <ul style="list-style-type: none"> Negotiation type—Type of phase 2 negotiation. The Junos OS currently supports quick mode. Message ID—Unique identifier for a phase 2 negotiation. Local identity—Identity of the local phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)</i>. Remote identity—Identity of the remote phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation)</i>. Flags—Notification to the key management process of the status of the IKE negotiation: <ul style="list-style-type: none"> caller notification sent—Caller program notified about the completion of the IKE negotiation. waiting for done—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. waiting for remove—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. waiting for policy manager—Negotiation is waiting for a response from the policy manager. 	detail

Sample Output

show services ipsec-vpn ike security-associations

```
user@host> show services ipsec-vpn ike security-associations
```

Remote Address	State	Initiator cookie	Responder cookie	Exchange type

192.0.2.1	Matured	062d291d21275fc7	82ef00e3d1f1c981	Main
192.0.2.2	Matured	cd6d581d7bb1664d	88a707779f3ad8d1	Main
192.0.2.3	Matured	86621051e3e78360	6bc5cc83fd67baa4	IKEv2
PIC: sp-0/3/0				
192.0.2.7	Matured	565e2813075e6fdb	67886757a74edcd6	IKEv2

show services ipsec-vpn ike security-associations detail

```

user@host> show services ipsec-vpn ike security-associations detail

IKE peer 198.51.100.2
  Role: Responder, State: Matured
  Initiator cookie: d91c9f20f78e1d4e, Responder cookie: 727a04ed8d5021a1
  Exchange type: IKEv2, Authentication method: Pre-shared-keys
  Local: 2013.0.113.2:500, Remote: 198.51.100:500
  Lifetime: Expires in 1357 seconds
  Algorithms:
    Authentication      : sha1
    Encryption          : 3des-cbc
    Pseudo random function: hmac-sha1
  Traffic statistics:
    Input bytes  :          22244
    Output bytes :          22236
    Input packets:           263
    Output packets:          263
  Flags: Caller notification sent
  IPsec security associations: 0 created, 0 deleted
  Phase 2 negotiations in progress: 0

IKE peer 192.0.2.4
  Role: Initiator, State: Matured
  Initiator cookie: cf22bd81a7000001, Responder cookie: fe83795c2800002e
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 192.0.2.5:500, Remote: 192.0.2.4:500
  Lifetime: Expires in 187 seconds
  Algorithms:
    Authentication      : md5
    Encryption          : 3des-cbc
    Pseudo random function: hmac-md5
  Traffic statistics:
    Input bytes  :          1000
    Output bytes :          1280
    Input packets:           5
    Output packets:           9
  Flags: Caller notification sent
  IPsec security associations: 2 created, 0 deleted
  Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 3582889153
  Local: 192.0.2.5:500, Remote: 192.0.2.4:500
  Local identity: ipv4_subnet(tcp:80,[0..7]=10.1.1.0/24)

```

```
Remote identity: ipv4_subnet(tcp:100,[0..7]=10.1.2.0/24)
Flags: Caller notification sent, Waiting for done
```

show services ipsec-vpn ike security-associations (on ACX500 Routers)

```
user@host> show services ipsec-vpn ike security-associations
```

Remote Address	State	Initiator cookie	Responder cookie	Exchange type
192.168.10.130	Matured	90864887dfecb178	9a2ee2ab786f960d	Main
192.168.20.130	Matured	1dd17732a8c9b13a	b06e5072ac7362bf	Main
192.0.2.7	Matured	565e2813075e6fdb	67886757a74edcd6	IKEv2

show services ipsec-vpn ipsec security-associations

Syntax `show services ipsec-vpn ipsec security-associations
<brief | detail | extensive>
<service-set service-set-name>`

Release Information Command introduced before Junos OS Release 7.4.

Description (Adaptive services interface only) Display IPsec security associations for the specified service set. If no service set is specified, the security associations for all service sets are displayed.

Options **none**—Display standard information about IPsec security associations for all service sets.

brief | detail | extensive—(Optional) Display the specified level of output.

service-set service-set-name—(Optional) Display information about a particular service set.

Required Privilege Level view

List of Sample Output [show services ipsec-vpn ipsec security associations extensive on page 1284](#)
[show services ipsec-vpn ipsec security associations detail on page 1285](#)
[show services ipsec-vpn ipsec security associations \(on ACX500 Routers\) on page 1285](#)

Output Fields [Table 85 on page 1281](#) lists the output fields for the **show services ipsec-vpn ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 85: show services ipsec-vpn ipsec security-associations Output Fields

Field Name	Field Description	Level of Output
Service set	Name of the service set for which the IPsec security associations are defined. If appropriate, includes the outside service interface VRF name.	All levels
Rule	Name of the rule set applied to the security association.	detail extensive
Term	Name of the IPsec term applied to the security association.	detail extensive
Tunnel index	Numeric identifier of the specific IPsec tunnel for the security association.	detail extensive
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels

Table 85: show services ipsec-vpn ipsec security-associations Output Fields (continued)

Field Name	Field Description	Level of Output
IPsec inside interface	Name of the logical interface hosting the IPsec tunnels.	All levels
Tunnel MTU	MTU of the IPsec tunnel.	All levels
Total uptime	Total amount of time that an IPsec tunnel has been up across security association rekeys.	detail
Local identity	<p>Protocol, address or prefix, and port number of the local entity of the IPsec association. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation). The protocol is always displayed as any because it is not user-configurable in the IPsec rule. Similarly, the port number field in the output is always displayed as 0 because it is not user-configurable in the IPsec rule. The value of the id-data-len parameter can be one of the following, depending on the address configured in the IPsec rule:</p> <ul style="list-style-type: none"> For an IPv4 address, the length is 4 and the value displayed is 3. For a subnet mask of an IPv4 address, the length is 8 and the value displayed is 7. For a range of IPv4 addresses, the length is 8 and the value displayed is 7. For an IPv6 address prefix, the length is 16 and the value displayed is 15. For a subnet mask of an IPv6 address prefix, the length is 32 and the value displayed is 31. For a range of IPv6 address prefixes, the length is 32 and the value displayed is 31. <p>The value of the id-data-presentation field denotes the IPv4 address or IPv6 prefix details. If the fully qualified domain name (FQDN) is specified instead of the address for the local peer of the IPsec association, it is displayed instead of the address details.</p>	All levels
Remote identity	<p>Protocol, address or prefix, and port number of the remote entity of the IPsec association. The format is id-type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation). The protocol is always displayed as any because it is not user-configurable in the IPsec rule. Similarly, the port number field in the output is always displayed as 0 because it is not user-configurable in the IPsec rule. The value of the id-data-len parameter can be one of the following, depending on the address configured in the IPsec rule:</p> <ul style="list-style-type: none"> For an IPv4 address, the length is 4 and the value displayed is 3. For a subnet mask of an IPv4 address, the length is 8 and the value displayed is 7. For a range of IPv4 addresses, the length is 8 and the value displayed is 7. For an IPv6 address prefix, the length is 16 and the value displayed is 15. For a subnet mask of an IPv6 address prefix, the length is 32 and the value displayed is 31. For a range of IPv6 address prefixes, the length is 32 and the value displayed is 31. <p>The value of the id-data-presentation field denotes the IPv4 address or IPv6 prefix details. If the fully qualified domain name (FQDN) is specified instead of the address for the remote peer of the IPsec association, it is displayed instead of the address details.</p>	All levels

Table 85: show services ipsec-vpn ipsec security-associations Output Fields (continued)

Field Name	Field Description	Level of Output
Primary remote gateway	IP address of the configured primary remote peer.	All levels
Backup remote gateway	IP address of the configured backup remote peer.	All levels
State	State of the primary or backup interface: Active , Offline , or Standby . Both ES PICs are initialized to Offline . For primary and backup peers, State can be Active or Standby . If both peers are in a state of Standby , no connection exists yet between the two peers.	All levels
Failover counter	Number of times a PIC switched between primary and backup interfaces, or the number of times the tunnel switched between the primary and remote peers since the software has been activated.	All levels
Direction	Direction of the security association: inbound or outbound .	All levels
SPI	Value of the security parameter index.	All levels
AUX-SPI	Value of the auxiliary security parameter index. <ul style="list-style-type: none"> When the value of Protocol is AH or ESP, AUX-SPI is always 0. When the value of Protocol is AH+ESP, AUX-SPI is always a positive integer. 	All levels
Mode	Mode of the security association: <ul style="list-style-type: none"> transport—Protects single host-to-host protections. tunnel—Protects connections between security gateways. 	detail extensive
Type	Type of security association: <ul style="list-style-type: none"> manual—Security parameters require no negotiation. They are static, and are configured by the user. dynamic—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode. 	detail extensive
State	Status of the security association: <ul style="list-style-type: none"> Installed—The security association is installed in the security association database. (For transport mode security associations, the value of State must always be Installed.) Not installed—The security association is not installed in the security association database. 	detail extensive
Protocol	Protocol supported: <ul style="list-style-type: none"> transport mode supports Encapsulation Security Protocol (ESP) or Authentication Header (AH). tunnel mode supports ESP or AH+ESP. 	All levels
Authentication	Type of authentication used: hmac-md5-96 , hmac-sha1-96 , or none .	detail extensive

Table 85: show services ipsec-vpn ipsec security-associations Output Fields (continued)

Field Name	Field Description	Level of Output
Encryption	Type of encryption algorithm used: can be 3des-cbc , aes-cbc (128 bits) , aes-cbc (192 bits) , aes-cbc (256 bits) , aes-gcm (128 bits) , aes-gcm(192 bits) , aes-gcm (256 bits) , des-cbc , or None . NOTE: In Junos FIPS mode, AES-GCM is not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, AES-GCM is supported in Junos FIPS mode.	detail
Soft lifetime Hard lifetime	Each lifetime of a security association has two display options, hard and soft, one of which must be present for a dynamic security association. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This information allows the key management system to negotiate a new SA before the hard lifetime expires. <ul style="list-style-type: none"> Expires in seconds seconds—Number of seconds left until the security association expires. Expires in kilobytes kilobytes—Number of kilobytes left until the security association expires. 	detail extensive
Anti-replay service	State of the service that prevents packets from being replayed: Enabled or Disabled .	detail extensive
SA lifetime	Configured hard lifetime (total lifetime), in seconds, for the security association.	detail
Replay window size	Configured size, in packets, of the antireplay service window: 32 or 64 . The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. If the replay window size is 0 , antireplay service is disabled.	detail
disable-natt	Configure to disable NAT-T functionality. By default the NAT-T is enabled.	All levels.
nat-keepalive	Specify the interval at which NAT keepalive packets can be sent so that NAT translation continues.	All levels.

Sample Output

show services ipsec-vpn ipsec security associations extensive

```
user@host> show services ipsec-vpn ipsec security-associations extensive
```

```
Service set: service-set-1
Rule: _junos_, Term: term-1, Tunnel index: 1
Local gateway: 192.0.2.2, Remote gateway: 198.51.100.4
IPSec inside interface: sp-2/0/0.1 Local identity:
ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Primary remote gateway: 192.0.2.1, State: Standby
Backup remote gateway: 198.51.100.4, State: Active
Failover counter: 1

Direction: inbound, SPI: 3743521590, AUX-SPI: 0
```



```

Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 23043 seconds
Hard lifetime: Expires in 23178 seconds
Anti-replay service: Enabled, Replay window size: 64

Direction: outbound, SPI: 2551045240, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 23043 seconds
Hard lifetime: Expires in 23178 seconds
Anti-replay service: Enabled, Replay window size: 64

disable-natt: No, nat-keepalive: 10

```

show services ipsec-vpn ipsec security associations detail

```

user@host> show services ipsec-vpn ipsec security-associations detail
Service set: ipsec-sset-0, IKE Routing-instance: default

Rule: ipsec-rule-0, Term: term0, Tunnel index: 1
Local gateway: 192.0.2.1, Remote gateway: 192.0.2.2
IPSec inside interface: ms-3/0/0.1, Tunnel MTU: 1500
UDP encapsulate: Disabled, UDP Destination port: 0
Local identity: ipv4_subnet(any:0,[0..7]=198.51.100.0/16)
Remote identity: ipv4_subnet(any:0,[0..7]=203.0.113.0/16)
NATT Detection: Not Detected, NATT keepalive interval: 0
Total uptime: 0 days 0 hrs 1 mins 4 secs

Direction: inbound, SPI: 4004530393, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
Soft lifetime: Expires in 27885 seconds
Hard lifetime: Expires in 28736 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

Direction: outbound, SPI: 1323638473, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
Soft lifetime: Expires in 27885 seconds
Hard lifetime: Expires in 28736 seconds
Anti-replay service: Enabled, Replay window size: 4096
Copy ToS: Enabled
Copy TTL: Disabled, TTL value: 64
SA lifetime: 28800 seconds

```

show services ipsec-vpn ipsec security associations (on ACX500 Routers)

```

user@host> show services ipsec-vpn ipsec security-associations

Service set: SS_1, IKE Routing-instance: Customer-1

Rule: rule_1, Term: 1, Tunnel index: 2
Local gateway: 192.168.1.11, Remote gateway: 192.168.10.130

```

```
IPSec inside interface: ms-0/2/0.8, Tunnel MTU: 1300
UDP encapsulate: Disabled, UDP Destination port: 0
  Direction SPI      AUX-SPI    Mode      Type      Protocol
  inbound  2204677182  0         tunnel    dynamic   ESP
  outbound  3015420439  0         tunnel    dynamic   ESP
```

Service set: SS_2, IKE Routing-instance: Customer-1

```
Rule: Customer-1_rule_1, Term: 1, Tunnel index: 1
Local gateway: 192.168.1.12, Remote gateway: 192.168.20.130
IPSec inside interface: ms-0/2/0.7, Tunnel MTU: 1300
UDP encapsulate: Disabled, UDP Destination port: 0
  Direction SPI      AUX-SPI    Mode      Type      Protocol
  inbound  2093089828  0         tunnel    dynamic   ESP
  outbound  2160146627  0         tunnel    dynamic   ESP
```

show services ipsec-vpn ipsec statistics

Syntax	<pre>show services ipsec-vpn ipsec statistics <brief detail> <remote-gw remote-peer-address> <service-set service-set-name></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>New fields added in Junos OS Release 10.0.</p>
Description	(Adaptive services interface only) Display IPsec statistics for the specified service set. If no service set is specified, the statistics for all service sets are displayed.
Options	<p>none—Display standard IPsec statistics for all service sets.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>remote-gw remote-peer-address—(Optional) Display IPsec statistics for an individual IPsec tunnel and an individual remote host.</p> <p>service-set service-set-name—(Optional) Display information about a particular service set.</p>
Required Privilege Level	view
List of Sample Output	<p>show services ipsec-vpn ipsec statistics detail on page 1289</p> <p>show services ipsec-vpn ipsec statistics remote-gw on page 1289</p> <p>show services ipsec-vpn ipsec statistics (on ACX500) on page 1289</p>
Output Fields	Table 86 on page 1287 lists the output fields for the show services ipsec-vpn ipsec statistics command. Output fields are listed in the approximate order in which they appear.

Table 86: show services ipsec-vpn ipsec statistics Output Fields

Field Name	Field Description	Level of Output
PIC	The physical interface on which the IPsec tunnel is configured.	All levels
Service set	Name of the service set for which the IPsec tunnel is defined.	All levels
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels
Tunnel index	Numeric identifier of the specific IPsec tunnel for the security association.	All levels

Table 86: show services ipsec-vpn ipsec statistics Output Fields (continued)

Field Name	Field Description	Level of Output
ESP statistics	Encapsulation Security Payload (ESP) statistics: <ul style="list-style-type: none"> • Encrypted bytes—Total number of bytes encrypted by the local system across the IPsec tunnel. • Decrypted bytes—Total number of bytes decrypted by the local system across the IPsec tunnel. • Encrypted packets—Total number of packets encrypted by the local system across the IPsec tunnel. • Decrypted packets—Total number of packets decrypted by the local system across the IPsec tunnel. 	All levels
AH Statistics	Authentication Header statistics: <ul style="list-style-type: none"> • Input bytes—Total number of bytes received by the local system across the IPsec tunnel. • Output bytes—Total number of bytes transmitted by the local system across the IPsec tunnel. • Input packets—Total number of packets received by the local system across the IPsec tunnel. • Output packets—Total number of packets transmitted by the local system across the IPsec tunnel. 	All levels
Errors	<ul style="list-style-type: none"> • AH authentication failures—Number of authentication header (AH) failures. An AH failure occurs when there is a mismatch of the authentication header in a packet transmitted across an IPsec tunnel. • ESP authentication failures—Number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets. • ESP Decryption failures—Number of ESP decryption failures. • Bad headers—Number of invalid headers detected. • Bad trailers—Number of invalid trailers detected. • Replay before window drops—Number of replay errors. A replay error is generated when a duplicate packet is received within the replay window. • Replayed pkts—Number of packets replayed. • IP integrity errors—Number of IP integrity errors. • Exceeds tunnel MTU—Number of times the tunnel maximum transmission unit (MTU) value was exceeded. • Rule lookup failures—Number of rule lookup failures. • No SA errors—Number of errors resulting from a missing security association (SA). • Flow errors—Number of flow errors. • Misc errors—Number of miscellaneous errors. 	All levels

Sample Output

show services ipsec-vpn ipsec statistics detail

```
user@host> show services ipsec-vpn ipsec statistics
```

```
PIC: sp-0/2/0, Service set: ss0
```

ESP Statistics:

```
Encrypted bytes:      0
Decrypted bytes:      0
Encrypted packets:    0
Decrypted packets:    0
```

AH Statistics:

```
Input bytes:          168
Output bytes:         168
Input packets:         2
Output packets:        2
```

Errors:

```
AH authentication failures: 0
ESP authentication failures: 0
ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
Replay before window drops: 0, Replayed pkts: 0
IP integrity errors: 0, Exceeds tunnel MTU: 0
Rule lookup failures: 0, No SA errors: 0
Flow errors: 0, Misc errors: 0
```

show services ipsec-vpn ipsec statistics remote-gw

```
user@host> show services ipsec-vpn ipsec statistics remote-gw 192.0.2.1
```

```
PIC: sp-3/1/0, Service set: service-set-2
```

```
Local gateway: 198.51.100.1, Remote gateway: 192.0.2.1, Tunnel index: 2
```

ESP Statistics:

```
Encrypted bytes:      0
Decrypted bytes:      0
Encrypted packets:    0
Decrypted packets:    0
```

AH Statistics:

```
Input bytes:          0
Output bytes:         0
Input packets:         0
Output packets:        0
```

Errors:

```
AH authentication failures: 0
ESP authentication failures: 0
ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
Replay before window drops: 0, Replayed pkts: 0
IP integrity errors: 0, Exceeds tunnel MTU: 0
Rule lookup failures: 0, No SA errors: 0
Flow errors: 0, Misc errors: 0
```

show services ipsec-vpn ipsec statistics (on ACX500)

```
user@host> show services ipsec-vpn ipsec statistics
```

PIC: ms-0/2/0, Service set: SS_1

ESP Statistics:

Encrypted bytes:	4121664
Decrypted bytes:	151584
Encrypted packets:	64162
Decrypted packets:	1579

AH Statistics:

Input bytes:	0
Output bytes:	0
Input packets:	0
Output packets:	0

Errors:

AH authentication failures:	0
ESP authentication failures:	0
ESP decryption failures:	0
Bad headers: 0, Bad trailers: 0	
Replay before window drops: 0, Replayed pkts: 0	
IP integrity errors: 0, Exceeds tunnel MTU: 0	
Rule lookup failures: 3, No SA errors: 0	
Flow errors: 0, Misc errors: 0	

PIC: ms-0/2/0, Service set: SS_2

ESP Statistics:

Encrypted bytes:	576
Decrypted bytes:	576
Encrypted packets:	6
Decrypted packets:	6

AH Statistics:

Input bytes:	0
Output bytes:	0
Input packets:	0
Output packets:	0

Errors:

AH authentication failures:	0
ESP authentication failures:	0
ESP decryption failures:	0
Bad headers: 0, Bad trailers: 0	
Replay before window drops: 0, Replayed pkts: 0	
IP integrity errors: 0, Exceeds tunnel MTU: 0	
Rule lookup failures: 0, No SA errors: 0	
Flow errors: 0, Misc errors: 0	

show system certificate

Syntax	<code>show system certificate</code> <code><certificate-id></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series, T Series routers, QFX Series, and OCX Series switches only) Display installed certificates signed by the Juniper Networks certificate authority.
Options	none —Display all installed certificates signed by the Juniper Networks certificate authority. certificate-id —(Optional) Display the details of a particular certificate.
Required Privilege Level	maintenance
List of Sample Output	show system certificate on page 1292 show system certificate (QFX Series) on page 1292
Output Fields	Table 87 on page 1291 lists the output fields for the show system certificate command. Output fields are listed in the approximate order in which they appear.

Table 87: show system certificate Output Fields

Field Name	Field Description
Certificate identifier	Unique identifier associated with a certificate. The certificate identifier is the common name of the subject.
Issuer Subject	Information about the certificate issuer and the distinguished name (DN) of the issuer, respectively: <ul style="list-style-type: none"> • Organization—Name of the owner's organization. • Organizational unit—Name of the owner's department. • Country—Two-character country code in which the owner's system is located. • State—State in the USA in which the owner is using the certificate. • Locality—City in which the owner's system is located. • Common name—Name of the owner of the certificate. • E-mail address—E-mail address of the owner of the certificate.
Validity	When a certificate is valid.
Signature algorithm	Encryption algorithm applied to the installed certificate.

Table 87: show system certificate Output Fields (continued)

Field Name	Field Description
Public key algorithm	Encryption algorithm applied to the public key.

Sample Output

show system certificate

```

user@host> show system certificate
Certificate identifier: Dallas-v3
  Issuer:
    Organization: Juniper Networks, Organizational unit: Juniper CA,
    Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas CA,
    E-mail address:ca@example.com
  Subject:
    Organization: Juniper Networks, Organizational unit: Juniper CA,
    Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas-v3,
    E-mail address:ca@example.com
  Validity:
    Not before: Mar 13 03:23:25 2004 GMT
    Not after: Mar 24 03:23:25 2014 GMT
  Signature algorithm: sha1WithRSAEncryption
  Public key algorithm: dsaEncryption

```

show system certificate (QFX Series)

```

user@host> show system certificate
Certificate identifier: Dallas-v3
  Issuer:
    Organization: Juniper Networks, Organizational unit: Juniper CA,
    Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas CA,
    E-mail address:ca@example.com
  Subject:
    Organization: Juniper Networks, Organizational unit: Juniper CA,
    Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas-v3,
    E-mail address:ca@example.com
  Validity:
    Not before: Mar 13 03:23:25 2004 GMT
    Not after: Mar 24 03:23:25 2014 GMT
  Signature algorithm: sha1WithRSAEncryption
  Public key algorithm: dsaEncryption

```


show system statistics arp

Syntax	show system statistics arp
Release Information	Command introduced in Junos OS Release 9.6 for EX Series switches.
Description	Display system-wide Address Resolution Protocol (ARP) statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Proxy ARP on an EX Series Switch</i> • <i>Verifying That Proxy ARP Is Working Correctly</i>

show system statistics arp

```

user@switch> show system statistics arp
arp:
  90060 datagrams received
  34 ARP requests received
  610 ARP replies received
  0 resolution request received
  0 unrestricted proxy requests
  0 restricted proxy requests
  0 received proxy requests
  0 unrestricted proxy requests not proxied
  0 restricted proxy requests not proxied
  0 datagrams with bogus interface
  0 datagrams with incorrect length
  0 datagrams for non-IP protocol
  0 datagrams with unsupported op code
  0 datagrams with bad protocol address length
  0 datagrams with bad hardware address length
  0 datagrams with multicast source address
  0 datagrams with multicast target address
  0 datagrams with my own hardware address
  0 datagrams for an address not on the interface
  0 datagrams with a broadcast source address
  294 datagrams with source address duplicate to mine
  89113 datagrams which were not for me
  0 packets discarded waiting for resolution
  0 packets sent after waiting for resolution
  309 ARP requests sent
  35 ARP replies sent
  0 requests for memory denied
  0 requests dropped on entry
  0 requests dropped during retry
  0 requests dropped due to interface deletion
  0 requests on unnumbered interfaces
  0 new requests on unnumbered interfaces
  0 replies for from unnumbered interfaces

```

```
0 requests on unnumbered interface with non-subnetted donor
0 replies from unnumbered interface with non-subnetted donor
```